We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

4,800
Open access books available

122,000
International authors and editors

135M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

CLARIVATE ANALYTICS BOOK CITATION INDEX INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

8

Secure Long-Distance Quantum Communication over Optical Fiber Quantum Channels

Laszlo Gyongyosi and Sandor Imre
Budapest University of Technology and Economics,
Department of Telecommunications
Hungary

1. Introduction

In today's communication networks, the widespread use of optical fiber and passive optical elements allows to use quantum key distribution (QKD) in the current standard optical network infrastructure. In the past few years, quantum key distribution schemes have attracted much study. The security of modern cryptographic methods, like asymmetric cryptography, relies heavily on the problem of factoring large integers (Rivest et al., 1978), (Schneier, 1996). In the future, if quantum computers become reality, any information exchange using current classical cryptographic schemes will be immediately insecure (Shor, 1994), (Shor, 1997). Current classical cryptographic methods are not able to guarantee long-term security. Other cryptographic methods, with absolute security must be applied in the future.

Cryptography based on the principles of quantum theory is known as *quantum cryptography* (Bennett et al., 1982), (Bennett & Brassards, 1984), (Bennett, 1992), (Imre & Balázs, 2005). Using current network technology, in order to spread quantum cryptography, interfaces must be implemented that are able to manage together the quantum and classical channels. The information-theoretic security of optical-fiber based quantum communication is the fundamental question of quantum cryptography. Quantum cryptographic schemes use photons as information carriers. The physical properties of photons make it possible to use quantum bits to realize unconditionally secure quantum communication over *long distances (*Duan et al., 2001) using the current standard optical fiber network. On the other hand, the success of secure long-distance quantum communications and global quantum key distribution systems depends strongly on the development of efficient quantum *repeaters* (Van Meter et al., 2009).

This chapter is organized as follows. First is a brief overview of the optical-fiber based QKD protocols. Then, we give a description of a QKD protocol designed for long-distance quantum communications between the quantum repeater nodes - called the DPS (Differential Phase Shift) QKD protocol. Next we show the results on the information-theoretic security analysis of DPS QKD protocol. Finally, we give an introduction to the quantum repeaters, then we summarize the results.

1.1 QKD for optical fibers

The safety of quantum cryptography relies on the no-cloning theorem. According to no-cloning theorem, any eavesdropping activity on the quantum channel necessarily perturbs the state of the qubits, thus Alice and Bob can detect the presence of Eve in the communication. In quantum cryptography Eve cannot clone the sent qubits perfectly, thus she has to use an ancilla quantum state, interact with the sent quantum state. This chapter will analyze the DPS QKD protocol, using efficient computational information geometric algorithms. The DPS QKD protocol was introduced for practical reasons, since the earlier QKD schemes were too complicated to implement in practice. The DPS QKD protocol can be an integrated part of current network security applications, hence it's practical implementation is much easier with the current optical devices and optical networks. Moreover, the DPS QKD protocol can be implemented in long-distance quantum communications, between the *quantum repeater* nodes. As follows, we will focus on this QKD scheme, however there are many other QKD schemes available, see (Branciard et al., 2005), (Dušek et al., 2006), (Hübel et al., 2007), (Gomez-Sousa & Curty, 2009), (Kwiat et al., 2001), (Niederberger et al., 2005), (Renner et al., 2005).

The DPS QKD scheme was designed to offer a well-implementable and more efficient practical solution with better key generation rates to realize quantum cryptography, than classical QKD approaches. As follows, it provides the best way to achieve long-distance QKD over optical-fiber quantum channels. In the DPS quantum cryptography protocol, the sender and the receiver use weak coherent state pulses, and logical bits are encoded in the relative phase of the pulses. The sender encodes every logical bit in two signals, and at the receiver's side, Bob use the two signals to decode the sent logical bit. The relevance of the DPS QKD protocol could have been increased dramatically in practical applications, since the differential phase shift QKD protocol is much more simpler in hardware design than the well known QKD protocols, such as BB84 or the Six-state QKD protocols. On the other side, contrary to it's easy implementation and it's much simpler working mechanism, the DPS QKD's protocol unconditional security is still not proven. The proposed geometrical analysis shows a method to quantify the secure key generation rate of the DPS QKD protocol, which is still missing from the literature. The possible attacks against the DPS protocol have been studied deeply. In this section we analyze the information-theoretical impacts of quantum cloner based attacks against the DPS QKD protocol.

As the most general attack against the protocol, we analyze coherent attacks, based on two different types of quantum cloner machines. The first section is organized as follows. First is a short brief on the DPS QKD protocol, and then we show the results on the information-theoretic security analysis of DPS QKD protocol. Finally, we summarize the results. In the second part of the chapter we discuss long-distance optical-fiber based quantum communications.

2. The DPS QKD protocol

In practical implementations of QKD protocols, Alice, the sender, uses weak coherent pulses (WCP) instead of a single photon source. As has been shown, WCP based protocols have a security threat, since an eavesdropper can perform a photon number splitting attack against the protocol (Inoue et al., 2003), (Honjo et al., 2004). These kinds of attacks are based on the fact that some weak coherent pulses contain more than one photon in the same polarization

state, which provides information to the eavesdropper without any disturbance. The DPS protocol is robust against such photon number splitting attacks in practice, however a theoretical lower bound on the security of the protocol is still missing from the literature (Inoue et al., 2003), (Honjo et al., 2004). The working mechanism of the DPS QKD protocol is based on the same idea as the B92 protocol (Bennett, 1992): even two non-orthogonal quantum states are sufficient to perform a secure quantum key distribution. In the DPS protocol, Alice encodes the logical bits in the phase of the pulses. If the phases are modulated by 0, then Alice sends a logical zero, and if the phase between the two pulses is π, then she encodes a logical one. If the relative phase between two pulses is 0, then Bob will detect 0, and similarly, if the phase between the two pulses is π, then he will obtain a logical 1.

In the sending process, Alice generates coherent states of the same intensity μ, and from these states she forms a sequence, as follows:

$$\Psi = \ldots \left| e^{i\varphi_{k-1}} \sqrt{\mu} \right\rangle \left| e^{i\varphi_k} \sqrt{\mu} \right\rangle \left| e^{i\varphi_{k+1}} \sqrt{\mu} \right\rangle \ldots = \ldots \left| \psi(k-1) \right\rangle \left| \psi(k) \right\rangle \left| \psi(k+1) \right\rangle \ldots , \tag{1}$$

where the phases can be set at 0 or π, hence for a logical zero we have $e^{i\varphi_k} = e^{i\varphi_{k+1}}$, and for a logical one, the difference between the two phases is π, and $e^{i\varphi_k} \neq e^{i\varphi_{k+1}}$. Since the logical bits are encoded in the phases between the signals, the k-th signal has relevance in the determination of both the k-th and $(k+1)$-th logical bits, hence $\Psi \neq \ldots \left| \psi(k-1) \right\rangle \otimes \left| \psi(k) \right\rangle \otimes \left| \psi(k+1) \right\rangle \ldots$, and this fact increases the complexity of any security analysis (Inoue et al., 2003), (Honjo et al., 2004). From this viewpoint, the DPS protocol has been analyzed by Takesue *et al.* (Takesue et al., 2005). In this section we show that the complexity of the DPS QKD protocol's security analysis can be decreased dramatically, using fast computational information geometric methods (Gyongyosi & Imre, 2010), (Gyongyosi & Imre, 2010a), (Nielsen et al., 2007), (Nielsen & Nock, 2008), (Nielsen & Nock, 2008a), (Nielsen & Nock, 2009).

The security of the DPS QKD protocol lies in the fact that the sender randomly prepares and sends to Bob two non-orthogonal quantum states, similarly to the B92 protocol (Bennett, 1992). The DPS QKD protocol geometrically can be modeled in the same way as the B92 protocol, however its implementation is much easier in practice, since the DPS QKD protocol does not require a bright reference pulse as does the B92 protocol (Bennett, 1992), (Inoue et al., 2003), (Honjo et al., 2004). In practical implementations the DPS scheme can be realized by WCP pulses with an average photon number less than 1, and the sent WCP pulse can be described by

$$\left\langle \alpha \right| - \alpha \left\rangle = e^{-2|\alpha|^2} \right. , \tag{2}$$

where $|\alpha|^2 = \mu \ll 1$ is the average photon number per pulse (Inoue et al., 2003), (Honjo et al., 2004). The B92 protocol uses the same $0, \pi$ modulation-scheme, however the B92 protocol practical implementation is more complicated than the DPS QKD's scheme (Inoue et al., 2003), (Honjo et al., 2004).

The general setup of the DPS QKD protocol is illustrated in Fig. 1. The time difference between the pulses is known at the receiver's device.

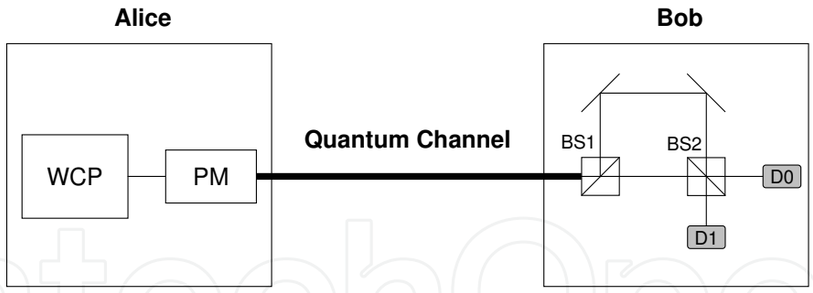

Fig. 1. A schematic view of DPS QKD protocol. Alice uses Weak Coherent Pulses (WCP) and a Phase Modulator (PM) to generate the signals. Bob decodes them with Beam Splitters (BS1, BS2) and photon detectors (D0, D1)

The optimal secure key rate of the protocol has been guaranteed only for individual attacks where the eavesdropper acts on the photons individually (Inoue et al., 2003), (Honjo et al., 2004). Here, we will analyze the most general collective attacker model, since the security of DSP QKD protocol against this general attack still remains an open question. In this attacker model, we analyze only the cloned photons from the given pulse, and we will give an approximation on the information obtainable by the eavesdropper. The analysis focuses on the eavesdropper's information about the given key, and the eavesdropper's cloned quantum states.

In the experimental realization of DPS QKD protocol, the signal consists of a weak coherent state and a strong phase reference. The relative optical phase between weak coherent state and reference pulse is either 0 or π, and these kinds of signals were already used in classical QKD schemes. In the attacker model, for simplicity we model these signals as two non-orthogonal quantum states, and we will analyze the still open questions related to the lower bounds on eavesdropper's obtainable information. As has been shown by Inoue (Agrawal, 1997) and Honjo (Honjo et al., 2004), the photon number splitting attacks can not be realized only with zero-error.

2.1 Practical quantum cryptography

Quantum cryptography uses the fundamental principles of quantum mechanics, and provides unconditionally secure communication. Optical channels have a fundamental role in quantum cryptography, since the information is encoded in the polarization states of photons.

The implementation of these quantum key distribution (QKD) schemes is much simpler than other approaches of quantum information processing, since these QKD schemes can be realized using the current optical network architecture. Quantum cryptography requires only the isolation of quantum states, unlike quantum computers, where the controlling of the interaction between quantum states is also a required task. In the case of quantum cryptography, the parties would like to communicate over macroscopic distances, hence optical fiber is a very practical choice to propagate and preserve the physical properties of photonic qubits (Paterson et al., 2004).

The experimental optical QKD schemes were intended to use single-photon sources and single-photon detectors, – but for practical reasons, many advanced classical optical

communication techniques have been integrated into these systems. Several experimental QKD solutions with different quantum information encoding approaches have been proposed since Bennett and Brassard introduced their scheme (Bennett & Brassard, 1984). The practical applications have brought out many question as to the security of different QKD schemes. By using optical fiber, it is possible to send the quantum states without decoherence. On the other hand, photon losses are still a significant issue in optical-fiber based quantum communications.

The decoherence of optical channels is often negligible in practice, however it may be critical in some practical implementations. The sent quantum states can easily be lost in the quantum channel, hence the sender has to resend the qubits. The losses in the optical fiber determine the speed of secret key generation and the information which can be leaked to an eavesdropper. The unconditional security of most optical-fiber based QKD protocols against sophisticated attacks is unquestionable; however the theoretical proof of this for all the QKD schemes is still missing. To develop a practical and unconditionally secure optical QKD scheme, it is necessary to maximize the maximal bridgeable distance and the speed of key generation (Duan et al., 2001).

One of the most important properties of all QKD schemes is that these protocols use standard telecommunication components and optical networks for their implementation. On the other hand, many attacks against the protocol can be achieved by these simple components, such as beamsplitter attacks, intercept-resend or photon number splitting attacks. A strict analysis of the efficiency of these methods is required to prove the security of practical quantum cryptography. The proposed method bridges the gap between information-theoretic proofs and the open questions regarding the security of practical QKD implementations. We can analyze the correlation between the information-theoretic security of the protocol and the length of the optical-fiber or the speed of secret key generation. The ideas and results that we present in this chapter can be useful for the analysis of the information-theoretic security of QKD and future quantum communication protocols and for studying the information-theoretic aspects of the security of quantum networks.

2.2 Demonstration of QKD

The first implementations of quantum cryptography were based on polarization encoding, hence the logical values of the qubits were encoded in the polarization angles of the photons and the communication distance was only a few tens of centimeters (Agrawal, 1997), (Townsend, 1997).

The optical-fiber channel based QKD was first demonstrated in 1993 by Townsend, Rarity and Tapster (Townsend, 1997). Their method was based on phase-coding, and the length of the optical fiber was 10 km. Later, optical-fiber based QKD was extended from phase-coding to polarization encoding (Galtarossa & Menyuk, 2005), however the communication was implemented only over a distance of 1.1 km. Later, many optical-fiber based QKD systems were demonstrated, such as the scheme presented by Dynes, (Dynes et al., 2007), Rosenberg (Rosenberg et al., 2007), and Villoresi (Villoresi et al., 2004). As a result of these demonstrations, with the help of optical quantum channels, quantum communication can now be implemented over large distances. In the following few years, many valuable research and results were demonstrated, and the speed of key generation and the

modulation techniques of the applied tools were increased dramatically. However, there are still many factors in real-life QKD implementations that add several imperfections to the working mechanism of the system (Kwiat et al., 2001).

However, as an important result of optical-fiber based QKD schemes, the photons which realize quantum states can be transmitted over long distances. The optical fibers make it possible to preserve the quantum states against the noise of the environment. In many practical long distance optical-fiber QKD systems, the information is rather encoded in the relative phase of two pulses, with very short time separation, since these encoding schemes can be applied more reliably for long-distance optical communications.

Currently, the longest transmission distance of optical-fiber based BB84 protocol is about 200 km, however advanced phase-modulation techniques make it possible to use the protocol over longer distances (Stucki et al., 2009), (Duan et al., 2001). QKD schemes were implemented over a 250 km long optical fiber, however these distances are still small compared to the distances in standard optical communication networks (Curty et al., 2008), (Inoue et al., 2003), (Honjo et al., 2004), (Kwiat et al., 2001), (Manderbach et al., 2007), (Takesue et al., 2005), (Stucki et al., 2009). The Six-state quantum cryptography protocol uses six polarization states to encode the logical bits in the qubits. The optical-fiber based Six-state QKD protocol tolerates more noise than the classical BB84 protocol (Kwiat et al., 2001), but its practical implementation requires more optical elements, which increases the noise in the system. Because of the greater noise level, the secret key generation rate of an optical-fiber based Six-state protocol is below that of the standard BB84 protocol. In the last few years many new optical-fiber based QKD approaches have been developed, such as the SARG04 protocol (Branciard et al., 2005), the Gaussian QKD scheme (Cerf et al., 2001), and the discrete-modulation QKD protocols (Inoue et al., 2003), (Honjo et al., 2004).

The DPS QKD scheme was designed to offer a more efficient practical solution with better key generation rates than classical QKD approaches (Honjo et al., 2004), (Inoue et al., 2003). In the DPS quantum cryptography protocol, the sender and receiver use weak coherent state pulses, and the logical bits are encoded in the relative phase of the pulses. The sender encodes every logical bit in two signals, and at the receiver's side, Bob use the two signals to decode the sent logical bit. The DPS QKD protocol has deep relevance to practical applications, since the differential phase shift QKD protocol is much simpler in hardware design than the well known QKD protocols, such as BB84 or the Six-state QKD protocols. Results on the security of DPS QKD protocol was published by Assche (Van Assche et al., 2004), Branciard, Gisin, and Scarani (Branciard et al., 2008), and several other attacks against various QKD schemes have been studied by Acín04 (Acín et al., 2004), Curty, Tamaki, and Moroder (Curty et al., 2008), Takesue et al. (Takesue et al., 2005), and Branciard et al. (Branciard et al., 2005), Curty et al. (Curty & Lütkenhaus, 2004), Fuchs et al. (Fuchs et al., 1997), Branciard, Devetak (Devetak & Winter, 2005), Cerf (Cerf et al., 2002), D'Ariano (D'Ariano & Macchiavello, 2003), Dušek (Dušek et al., 2006), Fasel (Fasel et al., 2004), Branciard (Branciard et al., 2005), and Gomez-Sousa and Curty (Gomez-Sousa & Curty, 2009), Hübel (Hübel et al., 2007), Niederberger (Niederberger et al., 2005), Renner05 (Renner et al., 2005).

The standard practical implementations of optical-fiber based QKD are bi-directional schemes, which means that the signal sent from Alice to Bob uses a bright carrier pulse, which was sent previously from Bob. The pulse travels from Bob to Alice, hence it can be

easily manipulated by an eavesdropper, who can perform an arbitrary operation on the pulse using her standard optical elements. Moreover, it is also possible to use her optical signals to replace the original signals sent by the legal parties.

Before we start to discuss the information-theoretic aspects of secure communication over optical-fiber based quantum channels, we give a short description of the physical properties of optical quantum channels.

3. Physical properties of optical quantum channels

In practical optical-fiber based quantum communication, the unitary transformations of the qubits are made by standard optical components such as beamsplitters, wave plates and phase shifters. These devices are sufficient for realizing all unitary transformations. Moreover, to send a qubit over long distances without the destruction and noise of the environment, the *current standard optical infrastructure* can be used.

In practical quantum cryptography the propagation of single photons over long-distance optical channels is still an exciting question, since the classical optical relay devices cannot be used anymore. In contrary to classical optical communications, in a quantum communication system the signal consists of individual quantum states, which, according to the no-cloning theorem, cannot be copied and repeated (Duan et al., 2001). The development of quantum repeaters that can handle quantum states is still under research, and it is impossible with current technology to amplify photons on the level of single quantum states. To describe the properties of optical quantum channels, we introduce the $\alpha \ db/km$ loss coefficient of the optical fiber channel, and the length L of the channel (Agrawal, 1997), (Townsend, 1997). For a fixed value of the loss coefficient $\alpha \ db/km$, the communication rate of the optical-fiber based QKD implementations can be analyzed as functions of the optical fiber length L. Many techniques have been developed to increase the efficiency of optical-fiber based quantum communication, such as increasing of photons per emitted pulse, but there are still many error correction and privacy amplification steps, which reduce further the speed of key generation. Currently, the fastest key generation speed in the standard BB84 QKD scheme was measured to be about 1.02 Mbps over a 20 km length optical fiber quantum channel (Niederberger et al., 2005). As we will show in Section 4.3, there is a connection between the radius of the smallest quantum informational ball and the fiber length (Gyongyosi & Imre, 2010).

In this section we discuss the optical fiber quantum channels. One of the most important questions from the security aspect of optical quantum channels is the loss of the optical channels. According to the no-cloning theorem, the quantum states sent cannot be repeated by a quantum repeater, hence the losses of the optical channel could cause many problems in practical communications. The level of loss determines the secret key generation rate and the maximal achievable transmission distance. From the viewpoint of the security of optical-based QKD, there is no difference between the quantum states lost in the quantum channel and the eavesdropped photons. In the security analysis, we have to count all the lost photons as eavesdropped qubits.

The relevance of optical fiber links for quantum communication was discovered by Agrawal et al (Agrawal, 1997). As has been shown, the loss in the optical fiber link mostly depends on the length L of the channel (Fasel et al., 2004), (Galtarossa & Menyuk, 2005), (Gomez-Sousa

& Curty, 2009), (Hübel et al., 2007). This length parameter affects the value of the transmission parameter *t* exponentially:

$$t = 10^{\frac{-\alpha L}{10}}, \tag{3}$$

where the parameter α determines the attenuation in dB/km. According to experimental results, this parameter depends on the wavelength used within the optical fiber, for a 1330 nm optical channel $\alpha \simeq 0.34\ dB/km$, and for 1550 nm it is about $\alpha \simeq 0.2\ dB/km$ (Fasel et al., 2004), (Galtarossa & Menyuk, 2005), (Hübel et al., 2007).

As has been shown by Fasel, Gisin, Ribordy, Zbinden (Fasel et al., 2004), there are two unavoidable effects in optical-fiber based communications, chromatic dispersion and polarization mode dispersion (Agrawal, 1997). Chromatic dispersion can be handled by optical elements, however the second phenomena cannot be compensated for, hence it can cause decoherence in polarization encoding based schemes. In recent optical fiber implementations, all of these effects can be suppressed and stable quantum communication can be implemented in practice (Gyongyosi & Imre, 2010).

Free-space optical quantum channels are mostly used in short-distance and ground-space links, and several free-space quantum channel implementations have been demonstrated in the past few years (Manderbach et al., 2007), (Villoresi et al., 2004). The attenuation of free-space optical channels is $\alpha < 0.1\ db/km$, and for an L length optical channel the transmission can be expressed in terms of the length and the attenuation of the channel as follows:

$$t \simeq \left[\frac{d_r}{d_S + DL}\right]^2 \cdot 10^{\frac{-\alpha L}{10}}, \tag{4}$$

where the parameters d_r and d_S are the apertures of the sending and receiving telescopes, and D is the divergence of the beam (Agrawal, 1997), (Galtarossa & Menyuk, 2005), (Hübel et al., 2007).

3.1 The effect of noise of quantum channels

Besides the fact that the Bloch sphere provides a very useful geometrical approach to describe the density matrices, it also can be used to analyze the noise of the optical fiber quantum channel models. From algebraic point of view, quantum channels are linear trace-preserving completely positive maps, while from a geometrical viewpoint, the quantum channel is an affine transformation. While, from the algebraic view the transformations are defined on density matrices, in the geometrical approach, the transformations are interpreted as Bloch vectors.

The image of the quantum channel's linear transform is an *ellipsoid* on the Bloch sphere (see Fig. 2). To preserve the condition for a density matrix ρ, the noise on the quantum channel $\mathcal{N}$ must be trace-preserving, i.e. $Tr\mathcal{N}(\rho) = Tr(\rho)$, and it must be completely positive, i.e. for any identity map *I*, the map $\mathcal{N} \otimes I$ maps a semi-positive Hermitian matrix to a semi-positive Hermitian matrix (Hayashi et al., 2005).

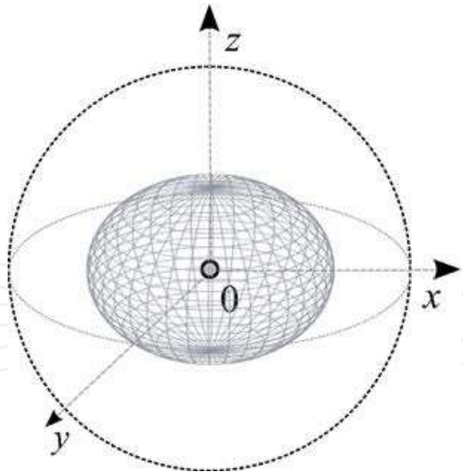

Fig. 2. Geometrically the image of the noisy quantum channel is an ellipsoid

We will use the terms "*unital*" and "*non-unital*" quantum channels. This distinction means the following thing: for a unital quantum channel $\mathcal{N}$, the channel map transforms the I identity transformation to the I identity transformation, while this condition does not hold for a non-unital channel. The optical fiber quantum channel belongs to the "non-unital" family (Hayashi et al., 2005).

To express it, for a unital quantum channel, we have $\mathcal{N}(I) = I$, while for a non-unital quantum channel, $\mathcal{N}(I) \neq I$. As we will see in Section 3.2, this difference can be rephrased in a geometrical interpretation, and the properties of the channel maps of the quantum channels can be analyzed using informational geometry. For a unital quantum channel, the center of the geometrical interpretation of the channel ellipsoid is equal to the center of the Bloch sphere. This means that a unital quantum channel preserves the average of the system states.

On the other hand, for a non-unital quantum channel, the center of the channel ellipsoid will differ from the center of the Bloch sphere. For an ideal enclosing scheme, the average of the pure orthogonal input states is equal to the center of the Bloch sphere. The main difference between unital and non-unital channels is that the non-unital channels do not preserve the average state. It follows from this that the numerical and algebraic analysis of non-unital quantum channels is more complicated than in the case of unital ones. While unital channels shrink the Bloch sphere in different directions with the center preserved, non-unital quantum channels shrink both the original Bloch sphere and move the center of the ball from the origin of the Bloch sphere. This fact makes our analysis more complex, however, in many cases, the physical systems cannot be described with unital quantum channel maps.

One of the most important quantum channels describing the transmission of information through optical-fibers, is *also a non-unital*.

Unital channel maps can be expressed as convex combinations of the four unitary Pauli operators (X, Y, Z and I), hence unital quantum maps are also called Pauli channels. Since the unital channel maps can be expressed as the convex combination of the basic unitary transformations, the unital channel maps can be represented in the Bloch sphere as different rotations with shrinking parameters. On the other hand, for a non-unital quantum map, the

map cannot be decomposed into a convex combination of unitary rotations and the transformation not just shrinks the ball, but also moves its center from the origin of the Bloch sphere.

The geometrical interpretations of a unital and a non-unital quantum channels are illustrated in Fig. 3.

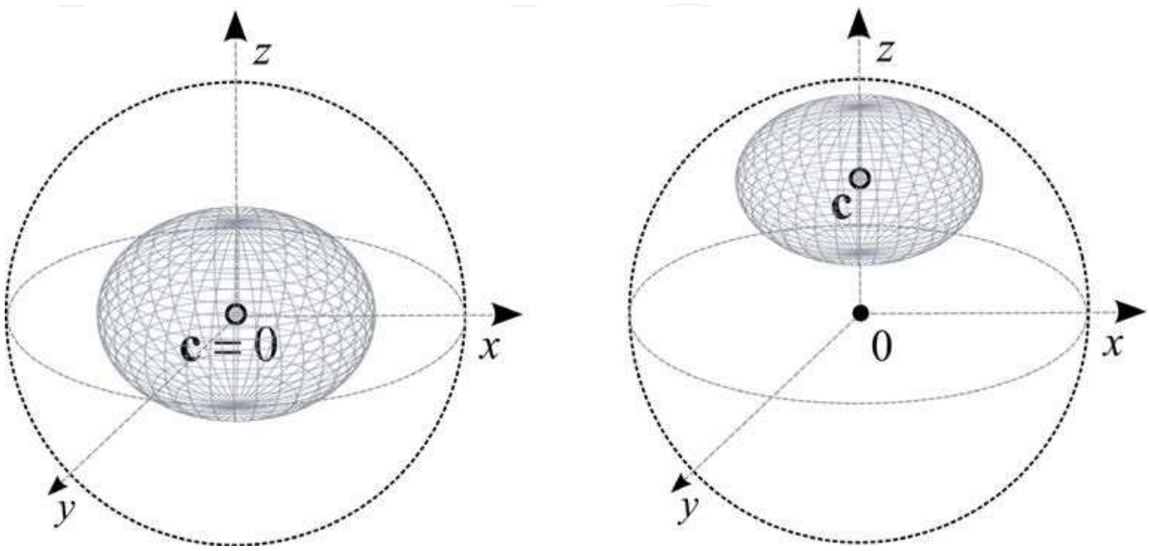

Fig. 3. The geometrical interpretation of a unital (a) and a non-unital (b) quantum channels

The unital channel maps can be expressed as convex combinations of the basic unitary transformations, while non-unital quantum maps cannot be decomposed into a convex combination of unitary rotations, because of the geometrical differences between the two kinds of maps. The geometrical approaches can help to reduce the complexity of the analysis of the different quantum channel models, and as we will show in Section 5, the problem of secure quantum communication over optical fiber channels can be converted into geometrical problems. The connection between the channel maps and their geometrical interpretation on the Bloch sphere makes it possible to give a simpler and more elegant solution for several hard, and still unsolved problems.

3.2 The noisy optical-fiber quantum channel

In this section, we introduce the general discussion of optical-fiber quantum channel - the amplitude damping channel. The effect of amplitude damping has great importance in optical communications, since this channel model describes energy dissipation. In practical optical or quantum communications, where quantum states or quantum bits are used, the loss of energy from the quantum system causes amplitude damping. In many practical applications, energy dissipation is an unavoidable phenomenon, and analysis of the amplitude damping quantum channel is therefore a relevant issue.

A non-unital amplitude damping quantum channel $\mathcal{N}$ can be described in the Kraus representation (Nielsen & Chuang, 2000), using a set of Kraus matrices $\mathcal{A}=\{A_i\}$, in the following form

$$\mathcal{N}(\rho)=\sum_i A_i \rho A_i^{\dagger}, \tag{5}$$

where $\sum_i A_i^{\dagger}\rho A_i = I$, and

$$A_1=\begin{bmatrix}\sqrt{p} & 0\\ 0 & 1\end{bmatrix}, \text{ and } A_2=\begin{bmatrix}0 & 0\\ \sqrt{1-p} & 0\end{bmatrix}, \tag{6}$$

where p represents the probability that the channel leaves the $|0\rangle$ input state unchanged. In practical optical-fiber based applications, this parameter represents the probability of energy loss from losing a particle. The channel flips the input state from $|0\rangle$ to $|1\rangle$ with probability $1-p$. If $p=0$, then the output of the channel is $|1\rangle$, with probability 1. For $|1\rangle$ input states, the channel leaves the input qubit untouched, and the output of the channel is $|1\rangle$ with probability 1. As can be concluded, the output of a non-unital amplitude damping quantum channel depends on the state of input qubit, and for, $p=0$, the channel output is $|1\rangle$ with probability 1.

For an optical quantum channel, the set of Kraus operators $\mathcal{A}=\{A_i\}$ can be transformed to the King-Ruskai-Szarek-Werner (KRSW) ellipsoid channel model (King & Ruskai, 2001), (Ruskai et al., 2001). In the KRSW channel model, the ellipsoid channel parameters are $\{t_k,\lambda_k\}$, where $k=1,2,3$. The analysis of non-unital channels is a more complicated task than for unital quantum channels since, in the KRSW representation, one or more parameters $\{t_k\}$ can be non-zero, which results in a more complicated calculation. The effect of $\{t_k\neq 0\}$ is that the average output $\rho=\sum_i p_i\rho_i$ of the channel moves away from the origin of the Bloch sphere, meaning that the center of the smallest enclosing quantum informational ball is not equal to the origin of the Bloch sphere $\frac{1}{2}I$. In the Bloch sphere representation, the effect of the amplitude damping channel on the initial input state $\rho=\frac{1}{2}\left(\mathbf{1}+|\mathbf{r}_{in}|\right)$, where $|\mathbf{r}_{in}|$ is the length of the initial Bloch vector, can be analyzed. The output state is denoted by $\mathcal{N}(\rho)=\frac{1}{2}\left(\mathbf{1}+|\mathbf{r}_{out}|\right)$, hence the amplitude damping channel can be expressed using Bloch vectors $\mathbf{r}_{in}$ and $\mathbf{r}_{out}$ in the following way:

$$\mathbf{r}_{out}=\begin{pmatrix}\mathbf{r}_{out}^{(x)}\\ \mathbf{r}_{out}^{(y)}\\ \mathbf{r}_{out}^{(z)}\end{pmatrix}=\begin{pmatrix}\sqrt{1-p} & 0 & 0\\ 0 & \sqrt{1-p} & 0\\ 0 & 0 & 1-\frac{p}{2}\end{pmatrix}\begin{pmatrix}\mathbf{r}_{in}^{(x)}\\ \mathbf{r}_{in}^{(y)}\\ \mathbf{r}_{in}^{(z)}\end{pmatrix}+\begin{pmatrix}0\\ 0\\ \frac{p}{2}\end{pmatrix}. \tag{7}$$

The amplitude damping channel performs an affine map on the input state and the effect of the channel can be visualized in the Bloch sphere representation. The optical-fiber quantum

channel can described in the KRSW ellipsoid channel model, with the following channel parameters (King & Ruskai, 2001), (Ruskai et al., 2001):

$$\begin{aligned} &t_x = 0,\ t_y = 0,\ t_z = 1-p, \\ &\lambda_x = \sqrt{p},\ \lambda_y = \sqrt{p},\ \lambda_z = p, \end{aligned} \tag{8}$$

where $p \in [0,1]$ is the channel parameter. In the Bloch sphere representation, the smallest value of $D(\rho\|\sigma)$ corresponds to the contour closest to the location of the density matrix.

In Figure 4(a), the Euclidean distances from the origin of the Bloch sphere to center $\mathbf{c}^*$ and to point ρ are denoted by m_σ and m_ρ, respectively. To determine the optimal length of vector $\mathbf{r}_\sigma$, the algorithm moves point σ. As we move vector $\mathbf{r}_\sigma$ from the optimum position, the larger contour corresponding to a larger value of quantum relative entropy D will intersect the channel ellipsoid surface, thereby increasing $\max_{\mathbf{r}_\rho} D(\mathbf{r}_\rho\|\mathbf{r}_\sigma)$. The optimal quantum informational ball is illustrated in light-grey in Figure 4(b). The first vector, m_σ, measures the Euclidean distance between the average and the center of the Bloch ball, while the second one, m_ρ, gives us the Euclidean distance from the center to the optimal channel output state.

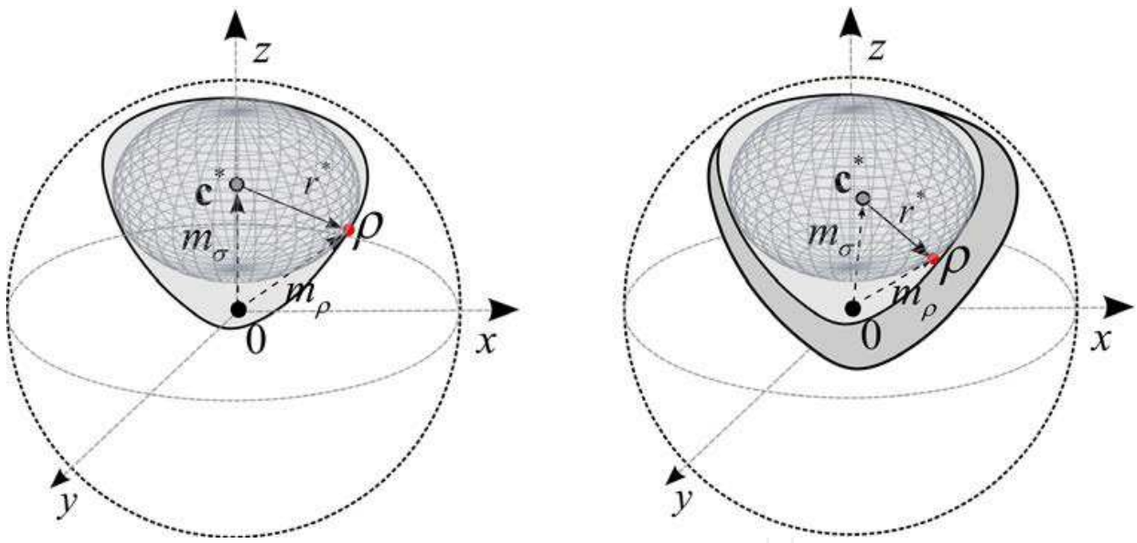

Fig. 4. Intersection of quantum informational ball and channel ellipsoid of optical-fiber quantum channel (a). As the vector moves from the optimal position, the quantum ball cannot be used to analyze the optical fiber quantum channel (b)

From a geometrical analysis, it can be concluded that the optimum input states for an optical-fiber quantum channel are unentangled, non-orthogonal quantum states (Gyongyosi & Imre, 2010a), (King & Ruskai, 2001), (Ruskai et al., 2001). The proposed geometrical approach - based on the quantum relative entropy function as distance measure between quantum states - has symmetries with the King-Ruskai-Szarek-Werner ellipsoid model (King & Ruskai, 2001), (Ruskai et al., 2001).

3.3 About the additivity of optical-fiber quantum channels

The additivity property of optical-fiber quantum channels is still an exciting subject of current research. There are some non-unital channels for which strict additivity is known, however the general rule for non-unital quantum channels is still not proven. The additivity of non-unital quantum channels is still an open question and currently under research. The additivity of optical quantum channels is still a remarkable and valuable research field in quantum information theory and it could have deep relevance to future quantum communications. The additivity of unital quantum channels is known and it has been proven that strict additivity holds for all unital quantum channels (Cortese, 2002). The fact that the optimum input states for an optical-fiber quantum channel $\mathcal{N}$ are unentangled, non-orthogonal quantum states, can be confirmed (King & Ruskai, 2001), (Ruskai et al., 2001). The geometrical analysis has shown that, for an optical-fiber quantum channel $\mathcal{N}$, there is no advantage in putting entangled quantum states to the input, and optimal results can be achieved by using non-orthogonal quantum states (Gyongyosi & Imre, 2010a). The average channel output state is denoted by σ, the center of the smallest quantum informational ball is denoted by $\mathbf{c}^*$. The geometrical analysis has shown that, for an optical-fiber quantum channel $\mathcal{N}$, there is no advantage in putting entangled quantum states to the input, and optimal results can be achieved by using non-orthogonal quantum states.

In Fig. 5, we show the smallest quantum informational balls with their radii vectors of amplitude damping channel $\mathcal{N}$ for orthogonal and non-orthogonal inputs. As it can be confirmed geometrically, the optimal channel capacity can be achieved by non-orthogonal input states.

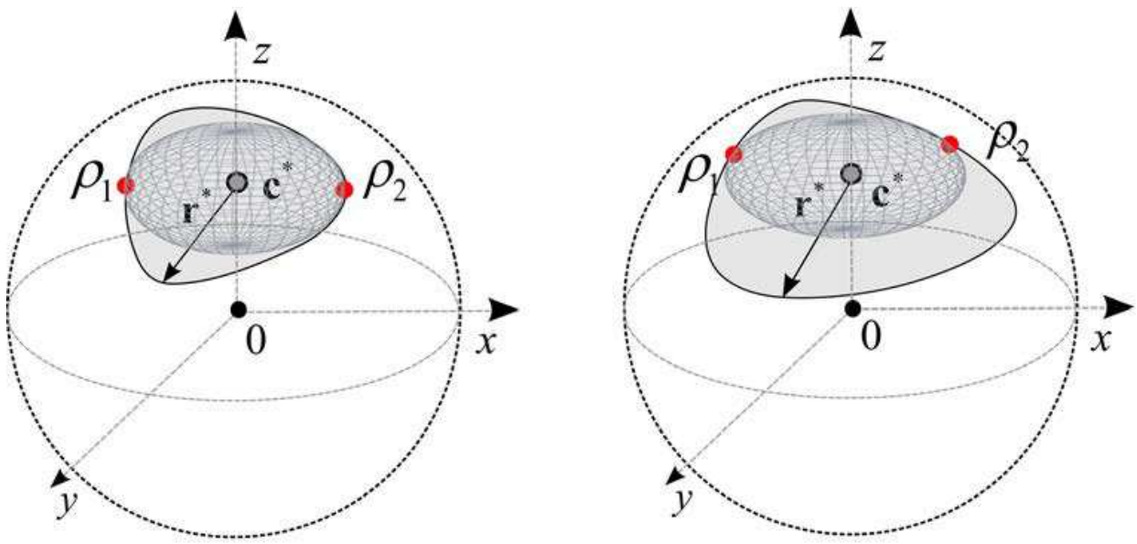

Fig. 5. The smallest quantum informational balls for amplitude damping channel model using orthogonal and non-orthogonal inputs

The optimal joint capacity of optical-fiber quantum channel $\mathcal{N}_{12} = \mathcal{N}_1 \otimes \mathcal{N}_2$, and the largest possible radius of the smallest enclosing quantum informational superball can be obtained by using non-orthogonal input states. The average channel state σ of the amplitude

damping channel $\mathcal{N}$ is located on the horizontal line between the optimal output states ρ_1 and ρ_2. As a conclusion, the average state σ of the channel ellipsoid is the average of the two optimal states ρ_1 and ρ_2. As follows, the optimal input states are not symmetric, hence these states are cannot be fitted to a horizontal line. The smallest quantum informational superball can be used to determine the optimal channel input states for which input states super-additivity holds. These states are asymmetric and hard to find them without this geometrical approach, using just a numerical analysis. The computation of the smallest quantum informational ball is based on quantum relative entropy function $D(\cdot\|\cdot)$, as distance measure.

4. Attacker models

This section analyzes the information-theoretic security of the most important practical optical-fiber based QKD protocols, such as BB84, the Six-state QKD protocol and the DPS QKD scheme. We analyze deeper the collective attacker model, since this attack can be considered as the most general attacker model. However, its physical realization requires many advanced devices, which are still not accessible for an eavesdropper, for future applications, a deep analysis of this attacker model would be appropriate and useful.

In the *individual* attacker model, the eavesdropper uses a probe and she entangles the sent quantum state and her probe state independently for every qubits. This model allows an eavesdropper to store her probes in quantum memory (Shuai et al., 2006) and she is able to measure the stored qubits independently, using the measurement information stolen from the steps of post-processing. Eve can combine the measurement strategies, she can apply POVM or standard von-Neumann measurements.

The *collective* attacker model, which is the subject of this section, is very similar to the individual attacker model. The eavesdropper is also able to use quantum memory to store the quantum states, however in this attacker model she is able to use a more advanced measurement strategy. In this case, Eve has the ability to use global generalized measurement on all the stored qubits as a single quantum state, using her advanced quantum computer. The collective attack is a more sophisticated and more surreptitious attack than the individual type of attack (as remarked already, the technological requisites are still missing for this). On the other hand, the theoretical analysis of this model would be very useful for the future.

In the attacker model analyzed here, the eavesdropper performs her attacks collectively on the qubits, and measures the stored quantum states using advanced measurement techniques and quantum computers. The general model of collective attack is illustrated in Fig. 6, the currently unavailable devices are colored in gray.

Finally, the third attacker model is the *coherent* attacker model. This model can be considered as the most general type of attack, since Eve can entangle the whole transmission with her probe of arbitrary dimensionality (Inoue et al., 2003), (Honjo et al., 2004).

For both type of attacks many security proofs exist, however the security of these QKD schemes in practice is still not shown, and is still an open question (Inoue et al., 2003), (Honjo et al., 2004). We give a very efficient information geometric approach to practically analyze the security of these protocols.

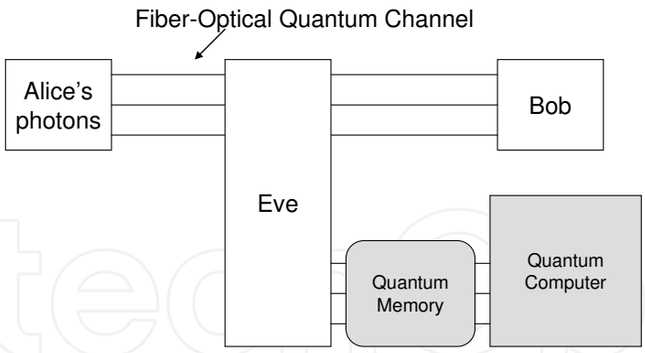

Fig. 6. The collective attacker model. The eavesdropper performs her attacks collectively on the qubits, and she measures the stored quantum states using advanced measurement techniques and quantum computers

4.1 Physically allowed cloning attacks for quantum cryptography

In secret quantum communications the best eavesdropping attacks on quantum cryptography are based on imperfect cloning machines. Using a probe, the eavesdropper imperfectly clones the sender's quantum state, keeps one copy, and sends the other. The physically allowed transformations of Eve's quantum cloner on Bob's qubit can be described in terms of Completely Positive (CP) trace preserving maps, which are affine map. The effects of a quantum cloner can be given in the tetrahedron representation (Gyongyosi & Imre, 2010a), (Hayashi, 2006).

Quantum cryptography is an emerging technology that offers new forms of security protection, however the quantum cloning based attacks against the protocol will play a crucial role in the future (Branciard et al., 2008), (Cerf et al., 2002), (Niederberger et al., 2005), (Townsend, 1997). We identify the quantum cloning based attacks in the quantum channel, and find potential and efficient solutions for their detection in secret quantum communications. The collective and coherent attacks against quantum cryptography are based on imperfect quantum cloners. The type of quantum cloner used depends on the quantum cryptography protocol. Against the Four-state (BB84) protocol, Eve, the eavesdropper, uses a phase-covariant cloner, while for the Six-state protocol, the optimal results can be achieved by the universal quantum cloner (UCM) (Biham & Mor, 1997), (Cerf et al., 2002), (Cerf, 2000), (Gyongyosi & Imre, 2010b), (Gyongyosi & Imre, 2010c), (Gyongyosi & Imre, 2010d). We use an efficient computational geometric method to analyze the quantum information theoretical impacts of physically allowed attacks on the quantum channel.

4.1.1 Preliminaries

In quantum cryptography the best eavesdropping attacks use the quantum cloning machines (Biham & Mor, 1997), (Cerf et al., 2002), (Cerf, 2000), (Gisin et al., 2001), (Gyongyosi & Imre, 2010b), (Gyongyosi & Imre, 2010c), (Gyongyosi & Imre, 2010d), (Nielsen & Chuang, 2000), (Yao, 1995). However, an eavesdropper can not measure the state $|\psi\rangle$ of a single quantum bit, since the result of her measurement is one of the single quantum system's eigenstates. The measured eigenstate gives only very poor information to the

eavesdropper about the original state $|\psi\rangle$. The process of cloning of *pure* states can be generalized as

$$|\psi\rangle_a \otimes |\Sigma\rangle_b \otimes |A\rangle_x \rightarrow |\Psi\rangle_{abx}, \tag{9}$$

where $|\psi\rangle$ is the state in the *Hilbert space* to be copied, $|\Sigma\rangle$ is a *reference* state, and $|A\rangle$ is the *ancilla* state (Bhar et al., 2007), (Gisin et al., 2001), (Nielsen & Chuang, 2000). A cloning machine is called *symmetric* if at the output all the clones have the same fidelity, and asymmetric if the clones have different fidelities.

The no-cloning theorem has important role in quantum cryptography, since it makes no possible to copy a quantum state perfectly. In 1996 Bužek and Hillery published the method of imperfect cloning, while the original no-cloning theorem was applied only to perfect cloning (Bužek & Hillery, 1996). The asymmetric cloning machines have been discussed for eavesdropping of quantum cryptography in (Cerf, 2000). For attacks on some quantum cryptography protocol, it has been proven that the best strategy uses quantum cloning machines (Cerf et al., 2002), (D'Ariano & Macchiavello, 2003). In this section we characterize the cloning machines by the *informational theoretical* meaning of quantum cloning activity in the quantum channel.

Alice's side is modeled by random variable $X = \{p_i = P(x_i)\}, i = 1,\ldots N$. Bob's side can be modeled by an other random variable *Y*. The Shannon entropy for the discrete random variable *X* is denoted by $H(X)$, which can be defined as $H(X) = -\sum_{i=1}^{N} p_i \log(p_i)$, for conditional random variables, the probability of the random variable *X* given *Y* is denoted by $p(X|Y)$. Alice sends a random variable to Bob, who produce an output signal with a given probability. Eve's cloner in the quantum channel increases the uncertainty in *X*, given Bob's output *Y*.

The general model for the quantum cloner based attack is illustrated in Fig. 7.

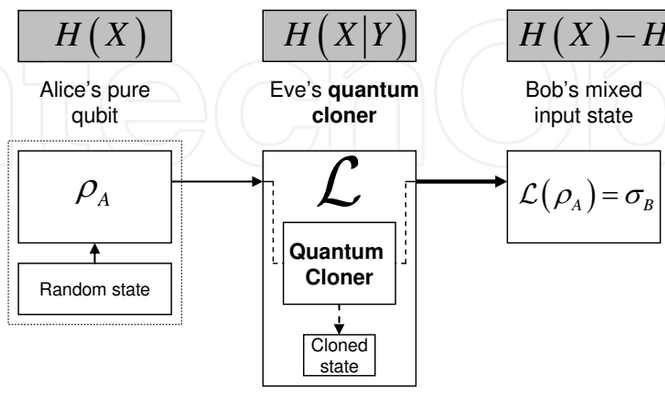

Fig. 7. The attacker model and the entropies

The informational theoretical noise of Eve's quantum cloner increases conditional Shannon entropy $H(X|Y)$, where

$$H\left(X|Y\right)=\sum_{i=1}^{N_X}\sum_{j=1}^{N_Y}p\left(x_i,y_j\right)\log p\left(x_i|y_j\right), \tag{10}$$

The security analysis is focused on the cloned mixed quantum state, received by Bob. The type of the quantum cloner machine depends on the actual protocol. For BB84, Eve chooses the phase covariant cloner (Rezakhani et al., 2005), while for the Six-state protocol she uses the universal quantum cloner (UCM) machine. Alice's pure state is denoted by ρ_A, Eve's cloner modeled by an affine map $\mathcal{L}$, and Bob's mixed input state is denoted by $\mathcal{L}\left(\rho_A\right)=\sigma_B$. We can use the fact, that for random variables X and Y, $H\left(X,Y\right)=H\left(X\right)+H\left(Y|X\right)$, where $H(X)$, $H\left(X,Y\right)$ and $H\left(Y|X\right)$ are defined by probability distributions.

We measure in a geometrical representation the information which can be transmitted in a presence of an eavesdropper on the quantum channel. The security of the quantum channel can be analyzed by *radius* r^* of the smallest enclosing ball of Bob, which describes the maximal transmittable information from Alice to Bob in the *attacked* quantum channel:

$$r^*=max_{\{all\ possible\ x_i\}}H\left(X\right)-H\left(X|Y\right). \tag{11}$$

To compute the radius r^* of the smallest informational ball of quantum states and the entropies between the cloned quantum states, instead of classical Shannon entropy, we will use von-Neumann entropy $\mathrm{S}(\cdot)$ and quantum *relative entropy* $D(\cdot\|\cdot)$ functions (Gyongyosi & Imre, 2010a). Geometrically, the presence of an eavesdropper causes a detectable mapping to change from a noiseless one-to-one relationship, to a stochastic map. If there is no cloning activity on the channel, then $H\left(X|Y\right)=0$, and the radius of the smallest enclosing quantum informational ball on Bob's side will be maximal (Gyongyosi & Imre, 2010).

4.1.2 Quantum cloning and QKD security

The security of QKD schemes relies on the *no-cloning* theorem (Bennett et al., 1982), (Wootters & Zurek, 1982). Contrary to classical information, in a quantum communication system the quantum information cannot be copied perfectly. If Alice sends a number of photons $|\psi_1\rangle,|\psi_2\rangle,\ldots,|\psi_N\rangle$ through the quantum channel, an eavesdropper is not interested in copying an arbitrary state, only the possible polarization states of the attacked QKD scheme. To copy the sent quantum state, an eavesdropper has to use a quantum cloner machine, and a known "*blank*" state $|0\rangle$, onto which the eavesdropper would like to copy Alice's quantum state. If Eve wants to copy the i-th sent photon $|\psi_i\rangle$, she has to apply a unitary transformation U, which gives the following result:

$$U\left(|\psi_i\rangle\otimes|0\rangle\right)=|\psi_i\rangle\otimes|\psi_i\rangle, \tag{12}$$

for each polarization states of qubit $|\psi_i\rangle$. A photon chosen from a given set of polarization states can only be perfectly cloned, if the polarization angles in the set are distinct, and are all mutually orthogonal (Cerf, 2000), (Wootters & Zurek, 1982). The unknown non-orthogonal states cannot be cloned perfectly, the cloning process of the quantum states is possible only if the information being cloned is classical. The polarization states in the QKD protocols are not all orthogonal states, which makes it impossible an eavesdropper to copy the sender's quantum states (Imre & Balázs, 2005), (Cerf, 2000), (Hayden et al., 2003),

(Wootters & Zurek, 1982). In the collective-type attacks, Eve imperfectly clones the sender's quantum state using her quantum state probe, she sends one copy to Bob and keeps the other copy. The effects of Eve's quantum cloner on Bob's qubit can be described in the terms of CP, trace preserving maps. The map of the quantum cloner compresses the Bloch-ball, as an affine map. This affine map has to be a complete positive, trace preserving map, which shrinks the Bloch ball along the *x, y* and *z* directions.

4.2 Inside a quantum cloner

This chapter strongly emphasizes the applicability of quantum cloners in secret quantum communications. In this section we see inside the quantum cloner using one of the most general quantum cloner models: the *universal* quantum cloner (Bhar et al., 2007), (Bužek & Hillery, 1996), (Hillery et al., 1999). The universal cloner produces two identical faithful copies of the input quantum state, and the quality of the output states is *independent* from the fidelity of the input state – hence it is really universal, as follows from its name. To describe the working mechanism of the universal quantum cloner, first we have to specific the inputs of the cloner machine. The input states of the quantum cloners are:

- the *original* unknown input quantum state,
- a *blank* quantum state onto which the unknown input state is to be cloned,
- and the state of the quantum cloner, which also can be referred to as the *ancilla state* or the *environment*.

The process of quantum cloning can be divided into two important parts:

- first part: *preparation* state,
- second part: *cloning* state.

In the first phase, the quantum cloner uses elementary single-qubit rotations, and CNOT transformations, while in the second phase only CNOT transformations are applied. It follows from this that the quantum circuit of a quantum cloner can be constructed from elementary quantum circuits, using simple quantum gates (Bhar et al., 2007).

The quantum circuit of an universal quantum cloner machine is illustrated in Fig. 8.

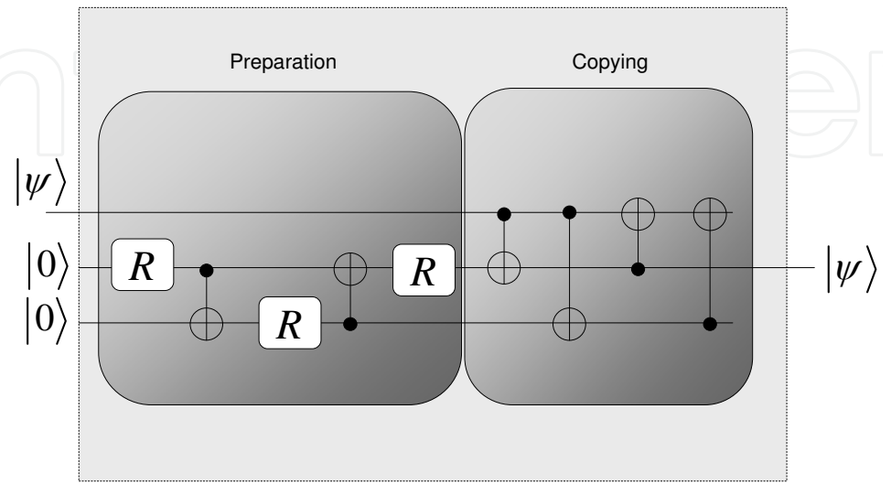

Fig. 8. Inside the universal quantum cloning circuit

The inputs of the quantum cloner are the unknown quantum state to be cloned, and the ancilla state: in this case, we have four dimensional ancilla, which represents the blank state for the copying and the environment of the quantum cloner machine. The blank state and the second ancilla state are known states—they are in the pure $|0\rangle$ state. The output of the quantum cloner machine consists of two clone quantum states and an ancilla state (Bhar et al., 2007).

4.3 Attacks against the DPS QKD protocol

To analyze the possible effects of an eavesdropper, - as in the previous case - we will use two kinds of quantum cloners, the most general universal quantum cloner and the phase covariant cloner. Other possible attacks against the protocol, such as sequential attacks, unambiguous state discrimination attacks or minimum error discrimination methods have been analyzed, and upper bounds have been obtained (Inoue et al., 2003), (Honjo et al., 2004). The security bounds for this type of attack were analyzed by Biham and Mor (Biham & Mor, 1997), and they have concluded the same bound holds for the protocol. In this attacker model, the eavesdropper tries to clone each of the quantum states sent by Alice, following an independent cloning strategy. The eavesdropper can change her strategy in a probabilistic way, hence in practical QKD applications, Eve can stop her cloning activity for a while, and then later, she can attack again. By changing the used strategies, she can decrease the probability of detection of her activity in the quantum channel.

In a collective attack, an eavesdropper can use a quantum memory to store her quantum states, and she can delay the whole measurement process. She can collect the required information from the steps of key agreement between Alice and Bob, which can be used to choose the best measurement strategy on the collected quantum states. As has been shown by Devetak and Winter (Devetak & Winter, 2005), the generic security bound for an collective attack can be given by the Csiszár–Körner bound (Csiszár & Körner, 1978) for one-way postprocessing as $I(A:B)-\min(I_{AE},I_{BE})$ with $I_{AE}=\max_{Eve}\chi(A:E)$, where I_E is the eavesdropper's information about the raw key of Alice and Bob, and $I(A:B)$ can be expressed as

$$H(A)+H(B)-H(AB). \tag{13}$$

To compute the χ *Holevo quantity*, we will use the fact, that this quantity can be expressed as the radius of the smallest enclosing quantum informational ball, hence

$$\begin{aligned} r^* &= I(A:E)=\mathrm{S}(E)-\mathrm{S}(E|A) \\ &= \max\chi(A:E)=\max\left(\mathrm{S}(\rho_E)-\sum_a p(a)\mathrm{S}\left(\rho_{E|a}\right)\right), \end{aligned} \tag{14}$$

where a is Alice's output with probability distribution $p(a)$, and $\rho_{E|a}$ is Eve's ancilla and $\rho_E=\sum_a p(a)\rho_{E|a}$ is the partial state of the eavesdropper. We note, that the same equation can be applied between Alice and Bob, when Bob is also able to store the quantum states.

The eavesdropper's most general strategy can include many possible variations which cannot be parameterized efficiently. However the security bounds for general or coherent attacks are the same as for collective attacks, hence the geometrical approach can be used to analyze both collective and coherent attacks. As has been shown by Branciard, Gisin, and Scarani (Branciard et al., 2008), the simplest realization of a collective attack against the DPS QKD protocol is the beam-splitting attack, hence here we use this type of attack to describe the informational-theoretic security of the DPS QKD protocol.

To describe the coherent beam-splitting attack, we model Alice's sent states as a sequence of coherent states $\otimes_i \left|\psi(i)\right\rangle$, where each $\psi(i)$ is chosen from the set $\{+\psi,-\psi\}$, and the logical value of the bit is 0 if $\psi(i-1)=\psi(i)$, and 1 if $\psi(i-1)=-\psi(i)$. In the collective beam-splitting attack, the eavesdropper uses a beamsplitter to get a fraction of the signal. The remaining fraction of the signal, denoted by τ, is sent directly to Bob, hence Bob will receive the state $\otimes_i \left|\psi(i)\sqrt{\tau}\right\rangle$, and similarly, the eavesdropper's state can be described as $\otimes_i \left|\psi(i)\sqrt{1-\tau}\right\rangle$. The eavesdropper's information can be given by using the von Neumann entropy, as

$$I_E^{DPS} = \mathrm{S}(\rho_E) - \frac{1}{2}\mathrm{S}\left(\rho_{E|0}\right) - \frac{1}{2}\mathrm{S}\left(\rho_{E|1}\right), \tag{15}$$

where it is assumed that the probability of each logical bit value is equal, hence

$$\rho_E = \frac{1}{2}\rho_{E|0} + \frac{1}{2}\rho_{E|1}\,. \tag{16}$$

Using the coding scheme $\psi(i-1)=\psi(i)$ for 0, and $\psi(i-1)=-\psi(i)$ for 1, the state of $\rho_{E|0}$ and $\rho_{E|1}$ can be expressed as

$$\rho_{E|0} = \frac{1}{2}P_{+\psi_E,+\psi_E} + \frac{1}{2}P_{-\psi_E,-\psi_E} \text{ and } \rho_{E|1} = \frac{1}{2}P_{+\psi_E,-\psi_E} + \frac{1}{2}P_{-\psi_E,+\psi_E}, \tag{17}$$

where $\psi_E = \psi\sqrt{1-\tau}$ and P_{ψ_E} is the projector. Using ψ_E, we can introduce a new parameter (Inoue et al., 2003), (Honjo et al., 2004)

$$\gamma = e^{-|\psi_E|^2} = e^{-\mu(1-\tau)}, \tag{18}$$

where μ is the intensity of the sent weak coherent pulse. Using this parameter, the inner product between $\left|\langle+\psi_E|-\psi_E\rangle\right| = \gamma^2$, for given μ intensity, the eavesdropper's information can be expressed as

$$\begin{aligned} I_E^{DPS}(\mu) &= 2H\left[\frac{\left(1-\gamma^2\right)}{2}\right] - H\left[\frac{\left(1-\gamma^4\right)}{2}\right] = \\ &2H\left[\frac{\left(1-\left|\langle+\psi_E|-\psi_E\rangle\right|\right)}{2}\right] - H\left[\frac{\left(1-\left|\langle+\psi_E|-\psi_E\rangle\right|^2\right)}{2}\right], \end{aligned} \tag{19}$$

where H is the Shannon entropy function.

The connection between the practically achievable secret key rate K of the protocol and the radius r^* of the smallest enclosing quantum informational ball of the eavesdropper can be given by (Inoue et al., 2003), (Honjo et al., 2004):

$$\begin{aligned} K(\mu) &= \left[I(A:B) - r^* \right] R = \left[I(A:B) - \max_{Eve} \left(\mathrm{S}(\rho_E) - \sum_a p(a) \mathrm{S}\left(\rho_{E|a}\right) \right) \right] R \\ &= v\left(1 - e^{-\mu\tau}\right)\left(1 - I_E^{DPS}(\mu)\right), \end{aligned} \tag{20}$$

where R is the raw key rate and v is the repetition rate.

5. Geometrical description of DPS QKD protocol

In phase-coding QKD schemes, a signal consists of a superposition of two time-separated pulses. These methods, instead of polarization encoding, encode the information in the relative phase between two pulses. However, the polarization and phase encoding schemes are equivalent mathematically (Inoue et al., 2003), (Honjo et al., 2004), hence in the information geometrical security analysis, we can use the Bloch-ball representation to study the security of the protocol. We can use the following translation between the basis states $|0\rangle$, $|1\rangle$ on the Bloch-ball, and the relative phases of the first signal $|S_1\rangle$, and the second signal $|S_2\rangle$:

$$\{|0\rangle, |1\rangle\} = \left\{ \frac{1}{\sqrt{2}}\left(|S_1\rangle + |S_2\rangle\right), \frac{1}{\sqrt{2}}\left(|S_1\rangle - |S_2\rangle\right) \right\}. \tag{21}$$

Hence for example, the $|\nearrow\rangle$ polarization state on the Bloch-ball can be rewritten in the following form:

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) = \frac{1}{\sqrt{2}}\left(|S_1\rangle + i|S_2\rangle\right). \tag{22}$$

In the case of $|\nearrow\rangle$, the relative phase between signals $|S_1\rangle$ and $|S_2\rangle$ is π. As we can conclude, the information encoded in the polarization and in the relative phases are equivalent.

In the analysis of the DPS QKD protocol, we can use the following conventions of the relative phases of the signals and the polarization states on the Bloch-ball:

$$\begin{aligned} &\frac{1}{\sqrt{2}}\left(|S_1\rangle + |S_2\rangle\right) = |0\rangle = |\leftrightarrow\rangle, \\ &\frac{1}{\sqrt{2}}\left(|S_1\rangle + i|S_2\rangle\right) = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) = |\nearrow\rangle. \end{aligned} \tag{23}$$

In Fig. 9, we have illustrated these conventions in the notations of the security analysis. The first and the second signals are denoted by $|S_1\rangle$ and $|S_2\rangle$.

The soundness of these notations of the proposed geometric analysis is based on the fact that the relative phases between the pulses can be represented by polarization angles on the

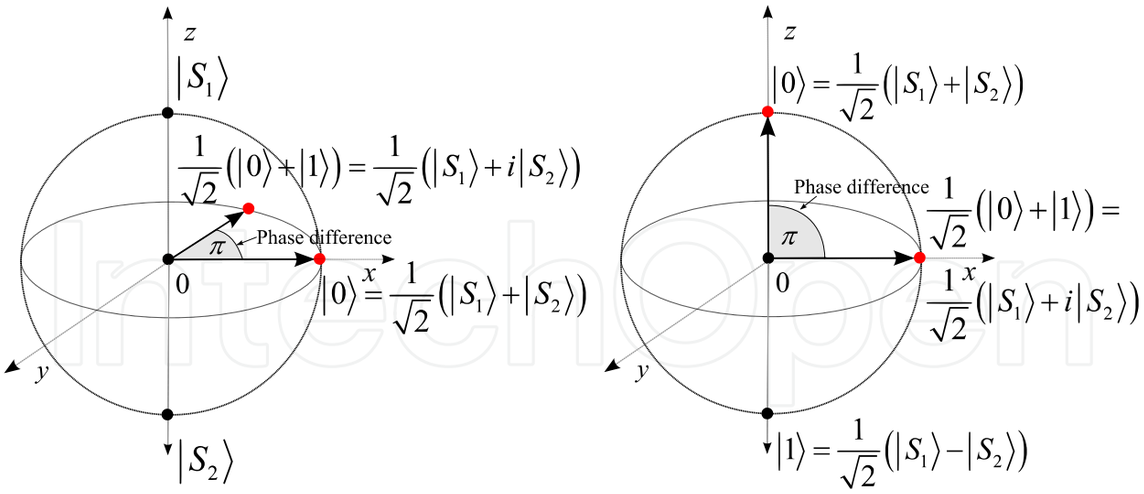

Fig. 9. The notations used in the geometrical analysis of DPS QKD protocol. The relative phases between the pulses can be represented by polarization angles on the Bloch-ball. The phase encoding and polarization encoding schemes are equivalent mathematically and in the geometrical security analysis

Bloch-ball, since the phase encoding scheme and the polarization encoding scheme are mathematically the same (Agrawal, 1997), (Inoue et al., 2003), (Gyongyosi & Imre, 2010), (Honjo et al., 2004). Hence, the DPS QKD protocol can be modeled in terms of the polarization states of the B92 protocol. It uses only two polarization states, and the key can be described by a random sequence $B=(b_1,b_2,\ldots b_N)$ of logical bits, and the generated N-length qubit string is:

$$|\psi\rangle=|\psi_{b_1}\rangle\otimes|\psi_{b_2}\rangle\otimes\ldots\otimes|\psi_{b_N}\rangle=\bigotimes_{i=1}^{N}|\psi_{b_i}\rangle, \tag{24}$$

where b_i is the basis of the i-th qubit. The i-th qubit $|\psi_{b_i}\rangle$ in the string is generated according to the B92 coding convention (Bennett, 1992), as $|\psi_0\rangle=|\leftrightarrow\rangle$ and $|\psi_1\rangle=|\swarrow\nearrow\rangle$.

In Fig. 10, we illustrated the two polarization states of the DPS QKD protocol, used in the information geometric security analysis.

In general, these polarization states can be expressed by means of some orthogonal basis $\{|0\rangle,|1\rangle\}$ as follows:

$$|\pm\alpha\rangle=a|0\rangle\pm b|1\rangle, \tag{25}$$

where the coefficients can be given by

$$a=\sqrt{\frac{1}{2}\left(1+e^{-2\mu_\alpha}\right)} \text{ and } b=\sqrt{\frac{1}{2}\left(1-e^{-2\mu_\alpha}\right)}, \tag{26}$$

and $a,b\in\mathbb{R}$ and $a^2+b^2=1$, and $a>b$ if $\mu_\alpha\neq 0$.

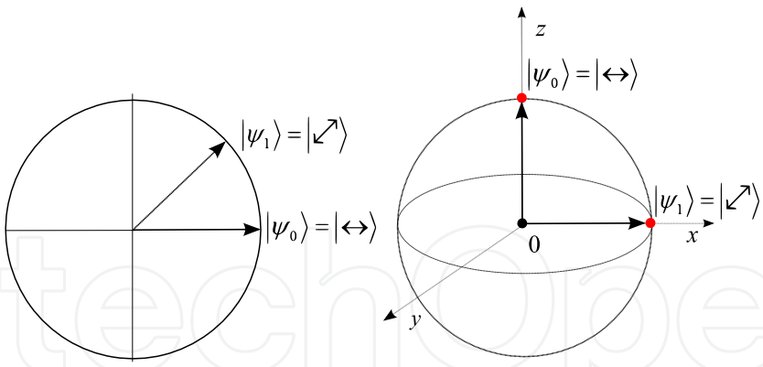

Fig. 10. The polarization states of the protocol

In Fig. 11, we show the polarization states of $|\pm\alpha\rangle = a|0\rangle \pm b|1\rangle$ in the Bloch-ball representation, and we depict the π phase difference between quantum states $\{|\rho_1\rangle, |\rho_2\rangle\}$ and $\{|\rho_3\rangle, |\rho_4\rangle\}$. In practice, Alice sends a WCP signal, whose phases are randomly modulated by 0 or π. These WCP signals are modeled by the quantum states $\{|\rho_1\rangle, |\rho_2\rangle\}$ and $\{|\rho_3\rangle, |\rho_4\rangle\}$ on the Bloch-ball.

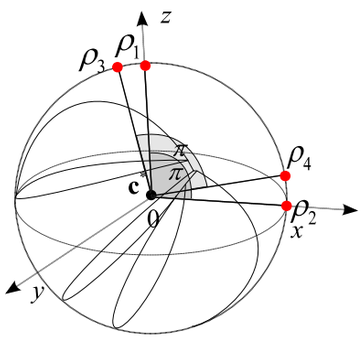

Fig. 11. The WCP pulses of DPS QKD protocol are modeled by different polarization states

In Fig. 12, we show the result of the eavesdropper's attack. For the best results, Eve uses the universal cloner for non-equatorial states ρ_1, ρ_2 and ρ_3, and the phase-covariant cloner for equatorial states (Bechmann-Pasquinucci & N. Gisin, 1999), (Cirac & Gisin, 1997), (Gyongyosi & Imre, 2010).

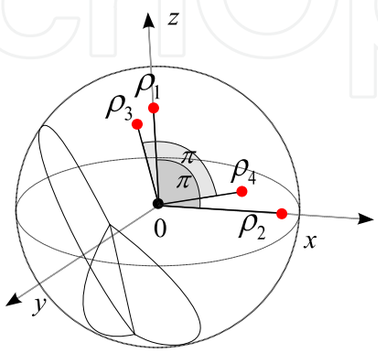

Fig. 12. The tessellation of the Bloch-ball for cloned quantum states differs from the diagram of the pure states originally sent

As can be concluded, the smallest enclosing quantum informational ball contains all the cloned states. The length of the radius of the smallest quantum informational ball describes the eavesdropper's maximally obtainable information.

In Fig. 13 we show the smallest enclosing quantum informational ball and the convex hull of the quantum states.

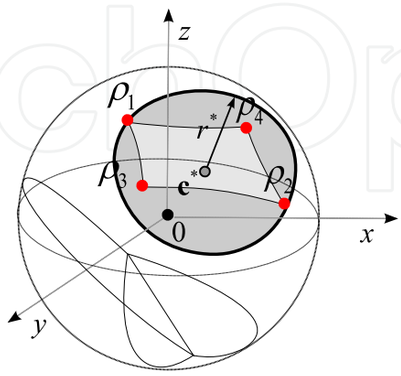

Fig. 13. The radius of the smallest quantum informational ball describes the eavesdropper's maximum obtainable information. The algorithm computes the length of the information-theoretical radius by the determination of the convex hull of mixed quantum states

We have computed the radius of the smallest quantum informational ball, which measures the information obtained by the attacker.

5.1 Coherent attack against the DPS QKD aprotocol

The DPS QKD protocol was introduced for practical reasons, since the earlier QKD schemes were too complicated to implement in practice. The DPS QKD protocol has high relevance to practice. The DPS QKD protocol can be integrated into current network security applications, hence its practical implementation is much easier with the current optical devices and optical networks. We introduce a fundamentally new method to analyze the information-theoretic security of the DPS QKD protocol.

To study the security of the protocol, we will analyze the collective attacker model against the optical-fiber based DPS QKD scheme. In this type of attack, Eve is equipped with beamsplitters, optical switch, detectors, quantum memory and a quantum computer (Biham & Mor, 1997), (Chen et al., 2006), (Gyongyosi & Imre, 2010a). As has been shown by Branciard, Gisin, and Scarani (Branciard et al., 2008), the simplest realization of a collective attack against the DPS QKD protocol is the beam-splitting attack, hence in this section we use this type of attack to describe the informational-theoretic security of the DPS QKD protocol.

The optical implementation and the optical devices of the eavesdropper's coherent attack are illustrated in Fig. 14.

Before we start to analyze the information-theoretic aspects of collective attacks against the optical-fiber based DPS QKD protocol, we give a short account of the parameters of photon detecting probabilities and the total efficiency of the quantum channel. As we have

explained previously, the single photon detection probability can be expressed as $p_{true} \approx \mu t$, where μ is the average number of photons per pulse and t is the total transmission efficiency of the optical fiber. We also use the quantum efficiency η of the receiver, and the loss of the detector of the receiver by $L_B \quad db/km$. The optical-fiber is characterized by its length L and its loss coefficient $\alpha \quad db/km$ (Branciard et al., 2005), (Duan et al., 2001).

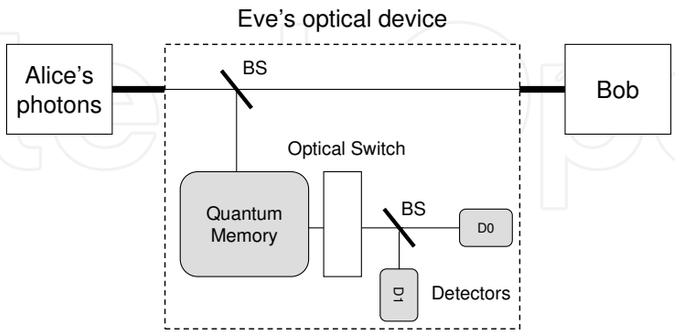

Fig. 14. Eve's optical device for coherent attack (BS-Beam Splitter)

Eve would like to calibrate her beamsplittered transmission to be equal to this t, however the sent beam with n_p pulses and with average photon number $n_p \mu t$ will be used by the eavesdropper. According to her strategy, she will use another beam with average photon number $n_p \mu (1-t)$, and the probability that the eavesdropper obtains the value of a logical bit at a certain time and Bob has also detected the photon, is $\mu (1-t)$.

In the collective attack, the eavesdropper can use a quantum memory, hence she is able to change her strategy, and she can store the pulses. However, the legal parties can delay the public announcement for an arbitrarily long time, hence the decoherence of the eavesdropper's quantum register makes it impossible to use the stored states (Biham & Mor, 1997). Moreover, as has been shown (Inoue et al., 2003), (Honjo et al., 2004), the eavesdropper can use an optical interferometer with an optical switch instead of a beamsplitter, hence the success probability of Eve can be increased to $2\left(\mu (1-t)\right)$. As a conclusion, using a beamsplitter, the eavesdropper is able to exactly determine the values of the bits for a fraction of the pulse which is $2\left(\mu (1-t)\right)$, and for the remaining $1-2\left(\mu (1-t)\right)$ fraction of the states, the eavesdropper enjoys only a 50% chance of getting the correct result. As has been shown (Agrawal, 1997), if the total transmission efficiency of the optical fiber is $t \ll 1$, then the mutual information between Eve and Bob is independent of this parameter, hence in this case it is independent of the transmission properties of the quantum channel. As one possible solution, the efficiency of the eavesdropper attack can be decreased, if the legal parties choose the average photon number μ to be small, independently of the total transmission efficiency of the optical fiber (Inoue et al., 2003), (Honjo et al., 2004).

5.2 Numerical results for the attacked DPS QKD protocol

In Fig. 15 we summarize the results for the proposed information geometric analysis of the security of the DPS QKD protocol against collective attacks. In Fig. 15(a), we introduced a new radius $r_{\sec ure} = I(A:B) - r^*$ derived from Eq. (20) and analyzed it in the function of the length of the optical fiber.

In Fig. 15(b), the secret key generation rate of the attacked quantum channel is derived from 15(a). The results are based on the analysis made above, and the properties of optical-fiber based quantum communication. In this model, Eve is equipped with a quantum memory, hence she is able to store the quantum states, which introduces a time delay in the communication (Chen et al., 2006), (Inoue et al., 2003), (Honjo et al., 2004). The analysis shows the correlation between the length of the optical fiber and the maximal secure key generation rate. The secret key generation rates are computed from the radius $r_{\sec ure}$ as a function of the fiber-length. The secure key generation rate was derived from the radius of the smallest quantum informational ball (Gyongyosi & Imre, 2010).

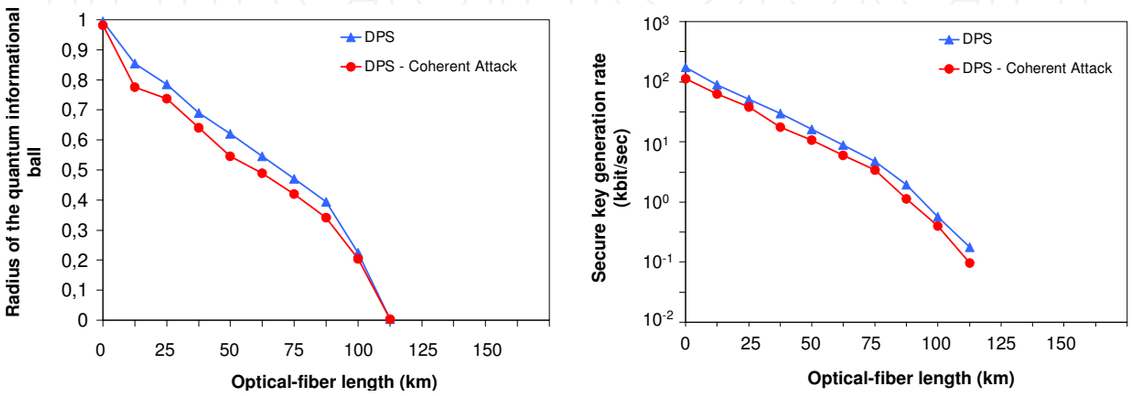

Fig. 15. Radii of the information-theoretic ball (a) and secure key generation rates (b) as a function of optical fiber length for DPS QKD protocols for an eavesdropper-free channel and an eavesdropped channel. The secret key rates are derived by the proposed information geometric algorithm

The secure key generation rate of the protocol for a coherent attack is computed from the radius of the quantum informational ball. It is slightly different from the result of the eavesdropper-free protocol, however there is no significant decrease in the radius of the smallest quantum informational ball (Gyongyosi & Imre, 2010).

In Fig. 16 we show the results of our analysis for a collective attack. The effects of the disturbance caused by the eavesdropper is analyzed in the range of $[0,0.5]$. The upper and lower bounds of radii of the eavesdropper's smallest quantum ball are shown as the function of the disturbance, using UCM and phase-covariant quantum cloners.

We have used the mutual information analysis to show the security of the DPS QKD protocol against coherent attacks. The radius of the smallest enclosing informational ball, hence the maximal obtainable information of the eavesdropper, increases with the level of disturbance. However, in the tolerated range of the disturbance level of the DPS QKD protocol, the analyzed quantum cloners make no possible for an eavesdropper to realize a successful attack in practice. As it is well described by the radii of the smallest quantum informational balls, the UCM based attack allows Eve less information than the phase-covariant based attack, which result confirms the mutual information analysis of UCM and phase-covariant cloner based attacks (Bechmann-Pasquinucci & N. Gisin, 1999), (Cirac & Gisin, 1997), (Gyongyosi & Imre, 2010).

The results of the information-theoretic based analysis confirmed the fact, that coherent attack does not help to Eve to increase her information about the key.

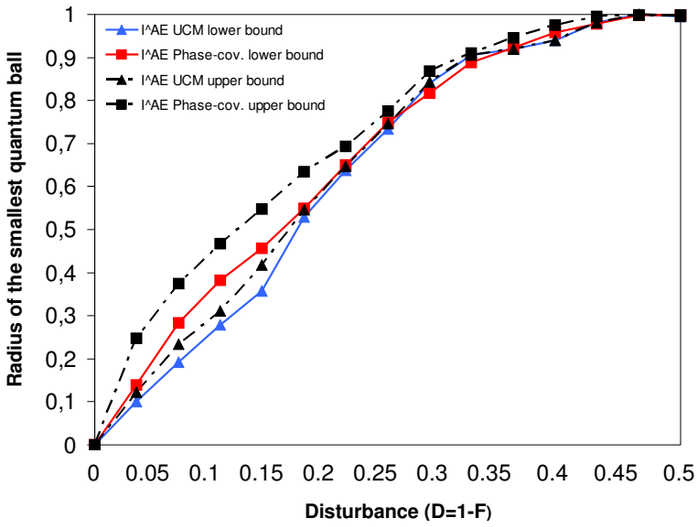

Fig. 16. Results of information geometrical security analysis of DPS QKD protocol for collective attack. The eavesdropper's obtainable information is described by the radius of the smallest enclosing quantum informational ball (lower bound - solid lines, upper bound - dashed lines)

5.2.1 Numerical results for the attacked DPS QKD protocol

The DPS QKD protocol offers information-theoretically secure quantum communication over optical fiber quantum channels, and the practical implementations of the protocol make it possible to use quantum cryptography in a simple and efficient way, with relatively high secret key generation rates over long distances. The protocol can be implemented easily with current optical network structure and optical fibers, and makes it possible for quantum cryptography to become a popular and easy-implementable practical cryptographic system in the future.

Practical QKD schemes require a reliable medium, which can transmit the photons with reasonable losses. The optical-fiber based QKD approaches seem to be the most appropriate choice for many practical reasons. This section analyzed the information-theoretic security of actual optical-fiber based QKD schemes using efficient information geometric approaches. In the proposed security analysis we introduced the smallest enclosing ball representation, which is used to describe the information-theoretic security of the QKD scheme. We analyzed the information-theoretic impacts of the most general eavesdropping attacks against the protocols, and we discovered the connection between the length of the optical fiber and the radius of the smallest enclosing quantum informational ball. Using the quantum informational ball representation, we derived the connection between the secret key generation rate over optical channels. The secure key rate is calculated from the information-theoretic radii of the smallest enclosing quantum informational balls, as a function of the length of the optical-fiber.

The proposed security analysis was focused on the most general coherent attack. Although sufficiently advanced technical devices—such as quantum memory or quantum computers—are still not available, the security of quantum communication against these attacks will be a very important issue in the future. To demonstrate the applicability of the

presented information geometric algorithm, we analyzed the information-theoretic security of the DPS QKD protocol.

6. Long-distance quantum communications with optical fiber channels

This chapter discusses secure long-distance quantum communications. As we have concluded in Section 5.2.1, the DPS QKD protocol can be the key protocol to achieve secure long-distance quantum communication over the optical-fiber based infrastructure. However, the secure long distance quantum communication would not be possible without the quantum repeater. In this section, we describe the working mechanism of quantum repeater, which is the key in the implementation of DPS QKD scheme over long distances with the help of the optical fiber network.

The success of future long-distance quantum communications and global quantum key distribution systems depends on the development of efficient quantum repeaters. A quantum repeater is not simply a signal amplifier, in contrast to classical repeaters. The quantum repeater is based on the transmission of entangled quantum states between the repeater nodes. As we will show in Section 6.1, there are several differences between a classical and a quantum repeater. In the quantum communication networks of the future, besides long distance communication, other networks structures could be implemented, such as self-organizing, truly probabilistic quantum networks, see (Gyongyosi & Imre, 2010e).

6.1 The quantum repeater

The quantum repeater nodes create highly entangled EPR (Einstein-Podolsky-Rosen) states with high fidelity of entanglement. The entangled quantum states can be sent through the quantum channel as single quantum states or as multiple photons. In the first case the fidelity of the shared entanglement could be higher, however it has lower probability of success in practice, since these quantum states can be lost easily on the noisy quantum channel (Duan et al., 2001). In order to recover fidelity of entanglement from noisy quantum states purification is needed. If the quantum repeaters could communicate with each other through idealistic quantum channels, the fidelity of the shared pairs would be nearly maximal, which could decrease dramatically the purification steps required.

Sharing of quantum entanglement plays critical role in quantum repeaters. The fidelity of the entanglement decreases during the transmission through the noisy quantum channel (Ladd et al., 2006), (Van Loock et al., 2008). Therefore, in practical implementations, the quantum entanglement cannot be distributed over very long distances; instead, the EPR states are generated and distributed between smaller segments (Van Meter et al., 2009).

A practical approach of the quantum repeater is called the “hybrid quantum repeater” (Van Meter et al., 2009), (Munro et al., 2008), (Jiang et al., 2008). The hybrid quantum repeater uses atomic-qubit entanglement and optical coherent state communication (Munro et al., 2010). In practice, the *base stations* of the quantum repeaters are connected by optical fibers, the entangled quantum states are sent through these fibers (Louis et al., 2008), (Sangouard et al., 2009).

Quantum repeaters use the purification protocol to increase the fidelity of transmission (Sangouard et al., 2009), (Stephens et al., 2008). The rate of entanglement purification

depends on the fidelity of the shared quantum states, since the purification step is a probabilistic process. Moreover, the success probability of the purification of the entangled quantum states depends on the fidelity of the entangled states – if the fidelity of entanglement of the shared state is low, then the success probability of its purification will be also low. Another important disadvantage of the purification algorithm is that it requires a lot of classical information exchange between the quantum nodes (Devitt et al., 2008).

The quantum repeater itself can be regarded as a quantum computer, which can realize the quantum teleportation algorithm and the purification steps. The quantum transformations at the receiver side of teleportation require classical inputs, since the quantum teleportation protocol uses them to recover the unknown quantum state from the entangled quantum state (Munro et al., 2010), (Louis et al., 2008), (Sangouard et al., 2009). In the sharing process, the sender base station entangles the quantum state with another separate physical qubit, and then it is multiplexed into the quantum channel (Van Meter et al., 2009). At the receiver's side, the multiplexed pulses are demultiplexed, and the receiver entangles each pulse with a free quantum state. If the entangling operation is successful, then the sender and the receiver share an EPR state (Duan et al., 2001), (Munro et al., 2010), (World Wide Science, 2011).

The entanglement creation uses the quantum communication channel; hence some noise is added to the transmitted states. As follows, in the next step, the created entanglement has to be purified (Bernardes et al., 2010), (Munro et al., 2010), (Van Meter et al., 2009). The purification is an error-correcting scheme, and it uses local quantum operations only – hence these operations can be realized in the separated base stations locally (Van Meter et al., 2009). The purification step takes two EPR pairs and by the usage of local quantum transformation and classical communication, it combines the two EPR states into one, higher-fidelity EPR pair (Munro et al., 2010).

In the next step, the unknown quantum state can be teleported by the quantum teleportation scheme, furthermore using entanglement swapping it can be transmitted to the final destination. The entanglement swapping (Munro et al., 2010), (Van Meter et al., 2009) is equal to a set of quantum teleportation steps – hence the entanglement swapping is an "extended teleportation protocol", which is able to bridge the gap between the physically separated stations in long distances (Duan et al., 2001), (Van Meter et al., 2009). During quantum teleportation, the sender's input quantum state is destroyed and recovered at the receiver's side, using shared entanglement between the parties. The receiver needs two classical bits to recover the unknown quantum state. In the protocol, both the sender and the receiver have to use local quantum operations only, which are based on classical information.

The purification process destroys the Bell pair, hence two quantum states in the middle station have been freed, and they can be reused in the next teleportation. The chain of repeaters has been constructed to extend of the distance between those nodes which share an EPR state. The purification scheme is able to correct the errors of the transmission which occurs at the node-switching and the fiber-based communication devices. The entanglement swapping can be extended to long distances, and by means of the node-to-node quantum communications, a global-scale quantum network can be constructed in the future (Van Meter et al., 2009).

In practical implementations, many EPR states can be shared between two nodes, and from these imperfect EPR pairs, the selection of the most appropriate pairs could be a complex algorithmic problem. In the literature several purification algorithms have been discussed, such as the symmetric purification, the pumping method, greedy scheduling or the banded purification method (Van Meter et al., 2008). The purification process is a probabilistic process, which means, that it can fail in some cases, but this probability decreases as the fidelity of the input EPR states grows (Van Meter et al., 2009).

6.2 The implementation of quantum repeaters

The design of a quantum repeater has been studied by Van Meter et al. (Van Meter et al., 2009), and in 2008 they presented a system design for a practical quantum repeater (Munro et al., 2008). Quantum repeaters will be very important for long-distance quantum communications, distributed quantum systems, and secure quantum communications. On the other hand, there are several differences between a classical and a quantum repeater. Due to the fundamental differences between the classical states and the quantum states, the quantum repeater works in a completely different way. The quantum repeater is not a signal amplifier, the way a classical repeater is.

The working mechanism of the quantum repeater is based on the following quantum protocols (Munro et al., 2008), (Van Meter et al., 2009):

- *purification of quantum states.*
- *entanglement swapping (quantum teleportation).*

The purification protocol is used to increase the fidelity of the distributed quantum states. Quantum teleportation is used to transport unknown quantum states using EPR states. Basically, these two quantum protocols represent the fundamental basis of a quantum repeater.

From an engineering point of view, the development of quantum repeaters is one of the biggest and most important challenges. As follows from the theoretical background of the quantum repeater, it requires a classical communication channel to assist the quantum communication. The quantum teleportation protocol requires classical information, otherwise the unknown quantum state cannot be recovered in a physically separated, distant location.

The quantum repeater uses quantum entanglement for the "retransmission" of a quantum state. We would like to guarantee the successful transfer of the quantum state, hence the implementation of an error correcting scheme is required. The quantum repeater will use the purification protocol, which can be used to increase the fidelity of the transmission.

In the work of Van Meter et al. (Van Meter et al., 2009), a new algorithm has been introduced for this purpose, they called it *banded purification* (Van Meter et al., 2009). The banded purification scheme could improve the utilization of the resources and the "repeating" of the quantum states.

The fidelity of the transmitted quantum states depends on the fidelity of the distributed EPR states. The entangled Bell states have to be shared among the stations in an initial step— these EPR states will be used in the teleportation protocol. After the EPR states have been

distributed and the teleportation of the unknown quantum state has been finished, an error-correction scheme has to be used to correct any possible errors produced during the transformation.

The quantum repeater itself is a quantum computer, which can realize the quantum teleportation algorithm and the purification steps. These quantum transformations require classical inputs, since the quantum teleportation protocol requires them.

Entanglement swapping is the process in which the quantum state repeats from A to B, through several intermediate base stations, using quantum teleportation and purification.

The working mechanism of the quantum repeater can be divided into the following main steps:

1. Creation of Bell states distributed among the quantum base stations,
2. Purification of the shared EPR states,
3. Teleportation between the nodes,
4. Entanglement swapping.

In a quantum communication network, the quantum repeater works differently from the classical repeater. The whole transmission rather could be called "entanglement swapping," since it is this step which realizes the transmission. Now, let's see the steps of the working mechanism of the quantum repeater.

In the first step, high-quality entangled pairs are shared between the base stations. These base stations could be a few tens of kilometers from each other. As has been shown by Van Meter et al. (Van Meter et al., 2009), using optical devices for quantum communication, the entangled quantum states can be created with a fidelity of 0.63 for 20 kilometers, which can even be increased by the purification step.

In the sharing process, the sender base station entangles a quantum state with another separate physical qubit, then it is multiplexed into the optical-fiber - or the quantum channel. At the receiver side, the multiplexed pulses are demultiplexed, and the receiver entangles each pulse with a free quantum state. If the entangling operation succeeds, then the sender and the receiver share an EPR state.

The process of entanglement creation between the base stations is illustrated in Fig. 17.

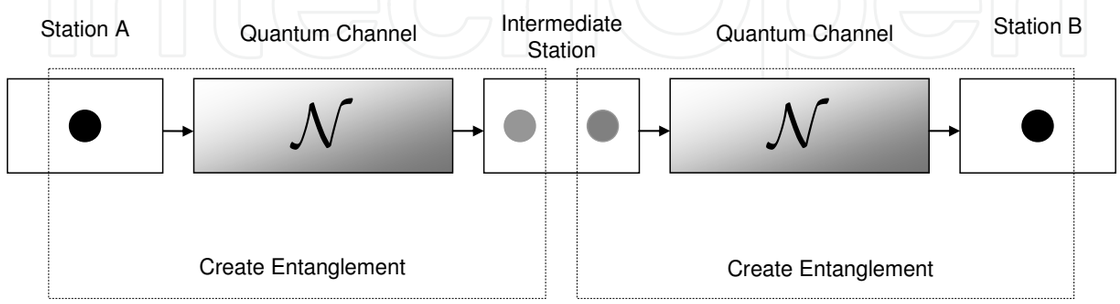

Fig. 17. The background of the quantum repeater is entanglement creation between the adjacent nodes. The quantum states are transmitted by quantum teleportation and local operations in the local nodes

The entanglement creation uses the quantum communication channel, hence some noise is added to the process. As follows, in the next step, the created entanglement has to be purified. The next step is purification, which can help to increase the fidelity of the shared EPR states before the unknown quantum state is teleported. The purification is an error-correcting scheme, and it uses local quantum operations only: hence these operations can be realized locally in the separated base stations (Van Meter et al., 2009).

Now, let's see what this purification does. The *purification* step takes two EPR pairs and by the use of local quantum transformation and classical communication, it combines the two EPR states into one EPR pair, which has greater fidelity.

The theoretical working mechanism of the purification step is illustrated in Fig. 18.

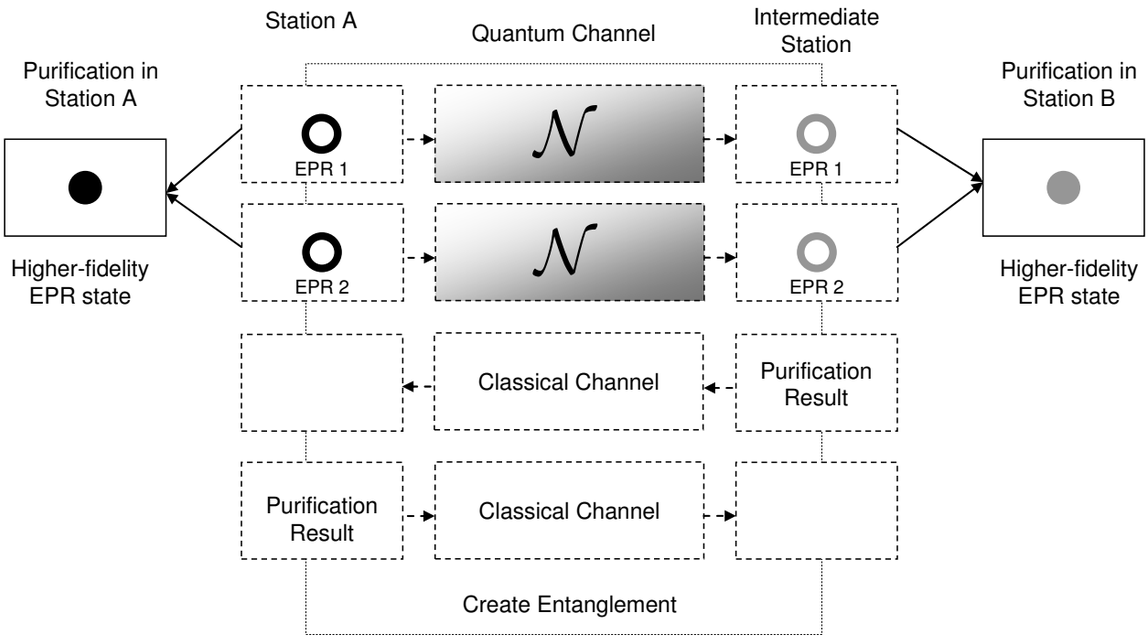

Fig. 18. The noisy quantum states can be purified by entanglement purification. This step requires a lot of resources and classical communication

The purification step has great relevance to the fidelity of the working mechanism of the quantum repeater, however the enhancement of the efficiency of this scheme is still under research (Munro et al., 2009). In the purification step, from two input EPR pairs one EPR pair is generated, hence the purification of the two EPR states destroys one EPR state. As follows, one EPR pair becomes a free qubit, hence this step frees some physical resources (Munro et al., 2009). The purification step could result in two possible outcomes:

1. the purification operation *fails*, and both EPR pairs are then freed;
2. the purification operation *succeeds*: the result is one EPR pair, with higher fidelity. If the fidelity is still low, this state can be used in the next purification step, otherwise it can be used for teleporting and entanglement swapping.

This purification can be done between several other EPR pairs, hence an efficient algorithm is required to choose the Bell pairs to be purified. This method is called *scheduling*, and it has

great importance from the viewpoint of the physical resources and the rate at which the fidelity of the shared EPR pairs can be increased (Bernardes et al., 2010).

After the purification step has been finished, in the next step the unknown quantum state can be teleported by the quantum teleporting scheme and by entanglement swapping it can be transmitted to its final destination (Bernardes et al., 2010).

The next step is teleportation and entanglement swapping. Entanglement swapping is equal to a set of quantum teleportation steps: hence entanglement swapping can be viewed as an "extended teleportation protocol," which is able to bridge the large distances between physically separated stations. The quantum teleportation protocol is a component of entanglement swapping, and while quantum teleportation is realized between base stations at short distances, entanglement swapping is an "extended teleportation" which is realized between the sender and the receiver stations. In the quantum teleportation scheme, Alice's input quantum state is destroyed and recovered at Bob's side, using shared entanglement between the parties. Bob needs two classical bits to recover the unknown quantum state. In this protocol, both Alice and Bob have to use local quantum operations only, which are based on classical information.

If we apply quantum teleportation between nodes at short distances, the final result will be referred as entanglement swapping. The Bell states are shared between the adjacent base stations, hence entanglement swapping has the following steps (Van Meter et al., 2009):

- entanglement sharing between Station 1 and Station 2,
- entanglement sharing between Station 2 and Station 3,
- teleportation from Station 1 to Station 2,
- local operations at Station 2, measurement of both quantum states: quantum bits are freed at Station 2,
- classical communication from Station 2 to Station 3,
- local operations at the Station 3.

This process destroys a Bell pair, hence two quantum states in the middle station have been freed, and they can be reused in the next teleportation. The result of the whole process is a swapped entanglement, which connects Station *A* and Station *B*.

As the result of the swapped entanglement, the unknown quantum state has been transferred from the sender base station to the receiver base station, through an arbitrary number of intermediate base stations. The structure of this quantum repeating consists of a chain of base stations—or quantum repeaters—and the information is transmitted via quantum teleportation. The chain of repeaters was constructed for the purpose of extending the distance between those nodes that share an EPR state. In the proposed construction this means that in the swapping process, two n-hop Bell pairs are combined into one $2n$ EPR state. This architecture is called the "doubling architecture" and, as has been shown by Briegel et al. (Briegel et al., 1998), the performance of the system declines polynomially rather than exponentially as the distance increases.

In the zero level of entanglement swapping, zero swaps has been made, in the first level one, while in the second level, two swap transformations have been realized. After the transformations have been finished, the initial EPR pair is stretched to reach all the hops, the EPR states of the intermediate hops—which mean three EPR states—have been destroyed (Van Meter et al., 2009).

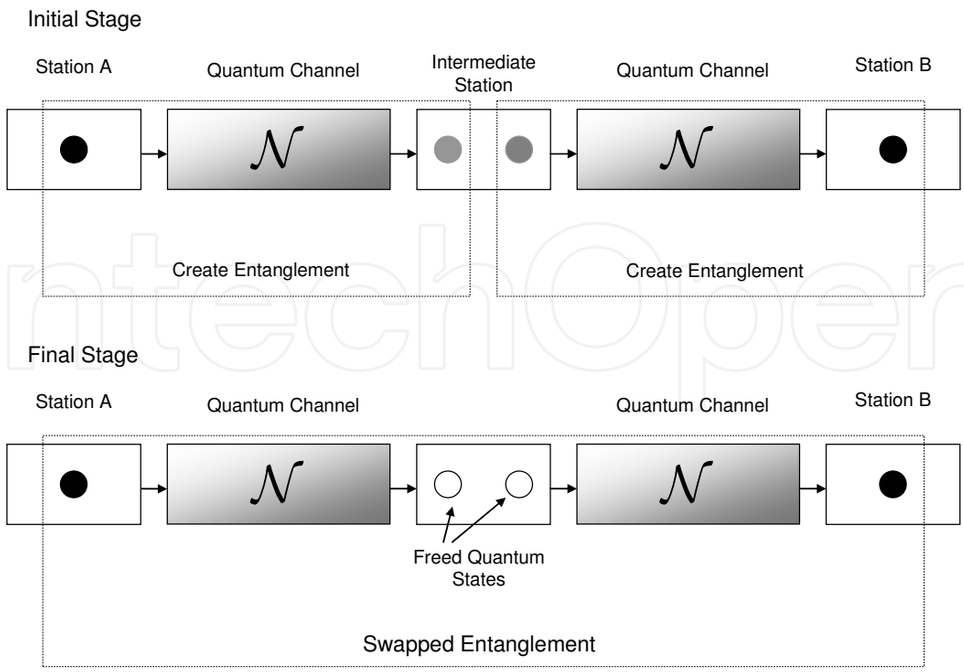

Fig. 19. The entanglement swapping realized by the local transformations made in the Intermediate Node. The swapping operation frees up the "intermediate" EPR states

The zero level of swapping with n base stations is illustrated in Fig. 20.

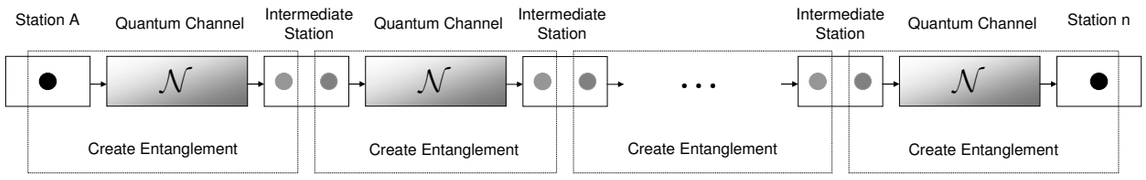

Fig. 20. In the first phase, the adjacent repeater nodes shares entanglement with each other

In this phase, each pair of adjacent base stations share an EPR pair with each other. In the next step, the adjacent base stations start to communicate with each other using quantum teleportation and classical communication. As a result of this step, the EPR state will span two base stations. The entanglement swapping will free up four quantum states.

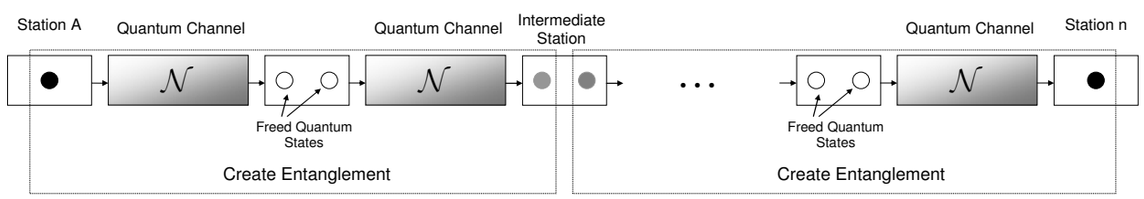

Fig. 21. After the EPR states have been shared, local transformations are made. These transformations free up quantum states in the nodes

In the second level, the entanglement swapping is realized between three base stations, which will result in four spanned base stations, and in six freed quantum states (Van Meter et al., 2009). The second level of entanglement swapping is illustrated in Fig. 22.

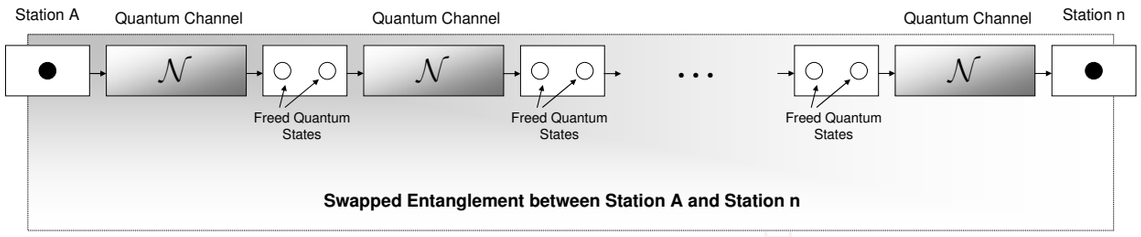

Fig. 22. After the local transformations have been realized in the intermediate stations, the result is an entanglement between node *A* and node *B*

The proposed method can be extended to n levels of entanglement swapping and the number of base stations spanned to 2^n. The architecture can be used for long-distance communication and in the quantum networks of the future (Munro et al., 2010), (Van Meter et al., 2009). Entanglement swapping is realized by the purification step and the quantum teleportation protocol combined with classical communications. The purification scheme is able to correct the errors of the transmission which occurs in the node-switching and the fiber-based communication devices. Entanglement swapping can be extended to long distances, and with the help of node-to-node quantum communications, a global scale quantum network can be constructed in the future.

7. Conclusion

In the first part of the chapter, we analyzed the DPS QKD scheme. The DPS QKD protocol has become more popular among quantum cryptographic protocols, since it offers higher key rates and easier implementation. The DPS protocol is tailored for practical applications—such as long-distance quantum communication over optical fiber quantum channels—and represents a more applicable protocol than other discrete- and continuous-variable QKD protocols, which were invented by theorists. The differential phase-shift protocol has better rates and its practical realizations are much simpler. However the security of the DPS QKD protocol is still an open question, since it unconditional security has not been fully approved yet. In this chapter, we analyzed the most general collective attack against the protocol by information geometrical methods, and for different attacker strategies. The proposed information geometrical method analyses the information-theoretic security of the DPS QKD protocol, and it could offer a very useful practical algorithmical solution to solve the still open and unknown questions related to the information-theoretic security of quantum cryptographic protocols. In the second part we have summarized the working mechanism of quantum repeater which will have great importance in optical fiber based secure long-distance quantum communications. The most ideal QKD protocol between the quantum repeater nodes should be the DPS protocol in the future, according to the flexibility, efficiency, easy implementability and low communication complexity.

8. Acknowledgment

The authors would like to thank the financial support from „*Sandor Csibi*" Ph.D. Researcher Scholarship at the Budapest University of Technology, Faculty of Electrical Engineering and Informatics, Hungary.

9. References

Acín, A.; Gisin, N.; Masanes, L. & Scarani, V. (2004). *Int. J. Quant. Inf.* 2, 23.

Agrawal, G. (1997). *Fiber-Optic Communication Systems* "Wiley, New York".

Bennett, C.H.; Brassard, G.; Breidbard, S. & Wiesner, S. (1982). Quantum cryptography, or unforgeable subway tokens. In D. Chaum, R. Rivest, and A. T. Sherman, eds., *Advances in Cryptology – Proc. CRYPTO '82* . Plenum Press.

Bennett, C.H. & Brassard, G. (1984). Quantum cryptography: public key distribution and coin tossing, Int. conf. Computers, Systems Signal Processing, Bangalore, India, December 10-12,175-179.

Bennett, C.H; (1992). Quantum cryptography using any two non orthogonal states, Phys. Rev. Lett. 68, 3121-3124.

Bernardes, N.K.; Praxmeyer, L. & van Loock, P. (2010). Rate analysis for a hybrid quantum repeater, arXiv:1010.0106v1.

Bhar, A.; Chattopadhyay, I. & Sarkar, D. (2007). No-Cloning and No-Deleting Theorems through the Existence of Incomparable States Under LOCC, *QUANTUM INFORMATION PROCESSING*, Volume 6, Number 2, 93-99, DOI: 10.1007/s11128-006-0041-2.

Biham, E. & Mor, T. (1997). Security of Quantum Cryptography against collective attacks, *Phys. Rev. Lett. 78* , 2256-1159.

Branciard, C.; Gisin, N. & Scarani, V. (2008). *New J. Phys*. 10, 013031.

Branciard, C.; Gisin, N.; Kraus, B. & Scarani, V. (2005). *Phys. Rev. A* 72, 032301.

Briegel, H.J.; Dür, W.; Cirac, I. & Zoller, P. (1998). Quantum repeaters: the role of imperfect local operations in quantum communication. *Physical Review Letters*, 81:5932 5935.

Bužek, V. & Hillery, M. (1996). Quantum copying: Beyond the no-cloning theorem, *Phys. Rev. A* 54, 1844–1852.

Cerf, N, Lévy. M. & Van Assche, G. (2001). *Phys. Rev. A* 63, 052311.

Cerf, N. (2000). Asymmetric quantum cloning machines in any dimension, *J.Mod.Opt.* 47 187, http://arxiv.org/abs/quant-ph/9805024.

Cerf, N.; Bourennane, M.; Karlsson, A. & Gisin, N. (2002). *Phys. Rev. Lett*. 88, 127902.

Cortese, J. (2002) "The Holevo-Schumacher-Westmoreland Channel Capacity for a Class of Qudit Unital Channels", LANL ArXiV e-print quant-ph/0211093.

Cirac, I. & Gisin, N. (1997) *Phys. Lett*. A, 229, 1.

Curty, M. & Lütkenhaus, N. (2004). *Phys. Rev. A* 69, 042321.

Curty, M.; Tamaki, K. & Moroder, T. (2008). *Phys. Rev. A* 77, 052321.

Csiszár, I. & Körner, J. (1978). *IEEE Trans. Inf. Theory 24*, 339.

D'Ariano, G. & Macchiavello, C. (2003). *Phys. Rev. A* 67, 042306.

Devetak, I. & Winter, A. (2005). Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A*, 461:207-235.

Devitt, S.J.; Munro, W.J. & Nemoto, K. (2008). High Performance Quantum Computing, arXiv:0810.2444.

Duan, L.; Lukin, M. D.; Cirac, J, I. & Zoller, P. (2001). "Long-distance quantum communication with atomic ensembles and linear optics," *Nature 414, 413*.

Dušek, M.; Lütkenhaus, N. & Hendrych, M. (2006). in *Progress in Optics*, edited by E. Wolf, "Elsevier, New York", Vol. 49, p. 381.

Dynes, J.; Yuan, Z. L.; Sharpe, A. W & Shields, A. J (2007) "Practical quantum key distribution over 60 hours at an optical fiber distance of 20km using weak and vacuum decoy pulses for enhanced security," *Opt. Express* 15, 8465.

Fannes, M. (1973). A continuity property of the entropy density for spin lattices. *Communications in Mathematical Physics*, 31:291.

Fasel, S.; Gisin, N.; Ribordy, G. & Zbinden, H. (2004). *Eur. Phys. J. D* 30, 143.

Fuchs, C.; Gisin, N.; Griffiths, R. B.; Niu, C.-S. & Peres, A. (1997). *Phys. Rev. A* 56, 1163.

Galtarossa, A., & Menyuk, C. R. (2005). Polarization Mode Dispersion (Springer, Berlin).

Gisin, N.; Ribordy, G.; Tittel, W. & Zbinden, H. (2001). Quantum cryptography. Quantph/0101098.

Gomez-Sousa, H. & Curty, M. (2009). *Quant. Inf. Comput.* 9, 62.

Gyongyosi, L. & Imre, S. (2010): Algorithmical Analysis of Information-Theoretic Aspects of Secure Communication over Optical-Fiber Quantum Channels, *Journal of Optical and Fiber Communications Research*, Springer New York, ISSN 1867-3007 (Print) 1619-8638 (Online).

Gyongyosi, L. & Imre, S. (2010): Information Geometrical Analysis of Additivity of Optical Quantum Channels, I*EEE/OSA Journal of Optical Communications and Networking (JOCN)*, IEEE Photonics Society & Optical Society of America, ISSN: 1943-0620; 2010.

Gyongyosi, L. & Imre, S. (2010): Algorithmic Superactivation of Asymptotic Quantum Capacity of Zero-Capacity Quantum Channels, *Information Sciences, Informatics and Computer Science Intelligent Systems Applications*, ELSEVIER, ISSN: 0020-0255; accepted. (In Press, 2011.).

Gyongyosi, L. & Imre, S. (2010): Information Geometrical Approximation of Quantum Channel Security, *International Journal On Advances in Security*, Published by: International Academy, Research and Industry Association, ISSN: 1942-2636.

Gyongyosi, L. & Imre, S. (2010): Quantum Singular Value Decomposition Based Approximation Algorithm, *Journal of Circuits, Systems, and Computers (JCSC)*, World Scientific, Print ISSN: 0218-1266, Online ISSN: 1793-6454.

Gyongyosi, L. & Imre, S. (2011). Quantum Cellular Automata Controlled Self-Organizing Networks, in "*Cellular Automata*", INTECH, ISBN 978-953-7619-X-X.

Bechmann-Pasquinucci, H. & Gisin, N. (1999). *Phys. Rev. A* 59, 4238.

Hayashi, M.; Imai, H.; Matsumoto, K.; Ruskai, M.B. & Shimono, T. (2005). Qubit channels which require four inputs to achieve capacity. *QUANTUM INF.COMPUT.*, 5:13.

Hayashi, M. (2006). *Quantum Information: An Introduction*. Springer-Verlag.

Hayden, P.; Leung, D.; Shor, P. & Winter, A. (2003). Randomizing quantum states: Constructions and applications. quant-ph/0307104.

Hillery, M.; Bužek, V. & Berthiaume, A. (1999). Quantum secret sharing. *Phys. Rev. A*,59:1829.

Honjo, T., Inoue, K. & Takahashi, H. (2004) Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit Mach-Zehnder interferometer, *Opt. Lett. 29,* 2797.

Hübel, H.; Vanner, R.; Lederer, T.; Blauensteiner, B.; Lorünser, T.; Poppe, A. & Zeilinger, A. (2007). *Opt. Express 15*, 7853.

Imre, S. & Balázs, F. (2005*): Quantum Computing and Communications – An Engineering Approach*, Published by John Wiley and Sons Ltd.

Inoue, K.; Waks, E. & Yamamoto, Y. (2003). Differential-phase-shift quantum key distribution using coherent light, *Phys. Rev. A* 68, 022317.

Jiang, L.; Taylor, J.M, Nemoto, K.; Munro, W.J.; Van Meter, R. & Lukin, M.D. (2008). *Quantum Repeater with Encoding*, arXiv:0809.3629.

King, C. & Ruskai, M. B. (2001). „Minimal entropy of states emerging from noisy quantum channels", *IEEE Trans. Info. Theory* 47, 192 - 209.

Kwiat, P.; Enzer, D. G.; Hadley, P. G. & Peterson, C. G. (2001). "Experimental Six-state quantum cryptography," in International Conference on Quantum Information, *2001 OSA Technical Digest Series* (Optical Society of America), paper FQIPB4.

Ladd. T.; van Loock, P.; Nemoto, K.; Munro, W.J. & Yamamoto, Y. (2005) .*New J. Phys*. 8, 184.

Louis, S.G.R.; Munro, W.J.; Spiller, T.P. & Nemoto, K. (2008). *Phys. Rev. A* 78, 022326.

Munro, W.J.; Harrison, K.A.; Stephens, A.M.; Devitt, S.J. & Nemoto, K. (2010). *Nature Photonics*, 10.1038/nphoton.2010.213.

Munro, W.J.; Van Meter, R.; Louis, S.G.R. & Nemoto, K. (2008). *Phys. Rev. Lett.* 101, 040502.

Niederberger, A.; Scarani, V. & Gisin, N. (2005). *Phys. Rev. A* 71, 042316.

Nielsen, M. & Chuang, I. L. (2000). *Quantum Computation and Quantum Information*, Cambridge University Press.

Nielsen, F.; Boissonnat, J-D. & Nock, R. (2007) On Bregman Voronoi diagrams. *In Proceedings of the 18th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'07),* pages 746–755, Philadelphia, PA, USA, Society for Industrial and Applied Mathematics.

Nielsen, F. & Nock, R. (2008). Bregman Sided and Symmetrized Centroids. *ICPR 2008*, *ICPR'08*, (arXiv:0711.3242).

Nielsen, F. & Nock, R. (2008). On the smallest enclosing information disk. *Inf. Process. Lett. IPL'08*, 105(3): 93-97.

Nielsen, F. & Nock, R. (2009). Approximating Smallest Enclosing Balls with Application to Machine Learning, International Journal on Computational Geometry and Applications (IJCGA'09).

Paterson, K.; Piper, F. & Schack, R. (2004). Why quantum cryptography?, eprint arXiv:quant ph/0406147.

Renner, R.; Gisin, N. & Kraus, B. (2005). *Phys. Rev. A* 72, 012332.

Rezakhani, A.; Siadatnejad, S.; Ghaderi, A. H. (2005). Separability in Asymmetric Phase Covariant Cloning, *Phys. Lett. A* 336, 278, 10.1016/j.physleta.2004.12.015, arXiv:quant ph/0312024v2.

Rivest, R.; Shamir, A. & Adleman, L. (1978). "A method for obtaining digital signatures and public-key cryptosystems." *Communications of the ACM* 21(2): 120-126.

Rosenberg, D.; Harrington, J. W.; Rice, P. R.; Hiskett, P. A.; Peterson, C. G.; Hughes, R. J. & Nordholt, J. E. (2007). "Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber," *Phys. Rev. Lett.* 98, 010 503.

Ruskai, M.; Szarek, S. & Werner, E. (2001). "An Analysis of Completely-Positive Trace Preserving Maps on 2 by 2 Matrices", LANL ArXiV e-print quant-ph/0101003.

Sangouard, N.; Simon, C.; de Riedmatten, H. & Gisin, N. (2009). Quantum repeaters based on atomic ensembles and linear optics arXiv:0906.2699.

Schmitt-Manderbach, T.; Weier, H.; FÄurst, M.; Ursin, R.; Tiefenbacher, F.; Scheidl, T.; Perdigues, J.; Sodnik, Z.; Kurtsiefer, C.; Rarity, J. G.; Zeilinger, A. & Weinfurter, H. (2007). "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km," *Phys. Rev. Lett.* 98, 010 504.

Schneier, B. (1996). *Applied Cryptography*. John Wiley & Sons.

Shor, P. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proc. 35th Ann. IEEE Symp. Foundations of Comp. Sci.*, pp. 124–134. IEEE Press, doi:10.1109/SFCS.1994.365700. eprint arXiv:quant-ph/9508027.

Shor, P. (1997). Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAMJ. Comp.,26(5):*1484-1509.

Shuai, C.; Yu-Ao, C.; Thorsten, S.; Zhen-Sheng, Y.; Bo, Z.; Jorg, S. & Jian-Wei, P. (2006). "Deterministic and Storable Single-Photon Source Based on a Quantum Memory." *Physical Review Letters 97*, 173004.

Stephens, A.M.; Evans, Z.W.; Devitt, S.J.; Greentree, A.D.; Fowler, A.G..; Munro, W.J.; O'Brien, J.L.; Nemoto, K. & Hollenberg, L.C.L. (2008). A Deterministic optical quantum computer using photonic modules, *Phys. Rev. A*. 78, 032318.

Stucki, D.; Walenta, N.; Vannel, F.; Thew, R. T.; Gisin, N.; Zbinden, H.; Gray, S.; Towery, C. R. & Ten, S. (2009). "High rate, long-distance quantum key distribution over 250km of ultra low loss fibers," *New J. of Phys.* 11, 075 003.

Takesue, H.; Diamanti, E.; Honjo, T.; Langrock, C.; Fejer, M.M.; Inoue, K.; & Yamamoto, Y. (2005). *New J. Phys.* 7, 232.

Townsend, P. (1997). Quantum cryptography on multiuser optical fiber networks," *Nature* 385, 47.

Van Assche, G.; Cardinal, J. & Cerf, N. J. (2004). *IEEE Trans. Inf. Theory* 50, 394.

Van Loock, P.; Lütkenhaus, N.; Munro, W.J. & Nemoto, K. (2008). *Phys. Rev. A* 78, 062319.

Van Meter, R.; Ladd, T.; Munro, W.J. & Nemoto, K. (2008). System Design for a Long-Line Quantum Repeater, arXiv:0705.4128v2 [quant-ph].

Van Meter, R.; Ladd, T.D.; Munro, W.J. & Nemoto, K. (2009). *IEEE/ACM Transactions on Networking* 17, 1002.

Villoresi, P.; Tamburini, F.; Aspelmeyer, M.; Jennewein, T.; Ursin, R.; Pernechele, C.; Bianco, G.; Zeilinger, A. & Barbieri, C. (2004). "Space-to-ground quantum-communication using an optical ground station: a feasibility study," arXiv:quant-ph/0408067v1.

Wootters, W. & Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*, 299:802 803, doi:10.1038/299802a0.

WorldWideScience.org (2011), Sample records for quantum computer development from *WorldWideScience.org*.

Yao, A (1995). Security of quantum protocols against coherent measurements. In *Proceedings of the 1995 ACM Symposium on Theory of Computing*, pages 67-75.

Optical Fiber Communications and Devices

Edited by Dr Moh. Yasin

ISBN 978-953-307-954-7
Hard cover, 380 pages
Publisher InTech
Published online 01, February, 2012
Published in print edition February, 2012

This book is a collection of works dealing with the important technologies and mathematical concepts behind today's optical fiber communications and devices. It features 17 selected topics such as architecture and topologies of optical networks, secure optical communication, PONs, LANs, and WANs and thus provides an overall view of current research trends and technology on these topics. The book compiles worldwide contributions from many prominent universities and research centers, bringing together leading academics and scientists in the field of photonics and optical communications. This compendium is an invaluable reference edited by three scientists with a wide knowledge of the field and the community. Researchers and practitioners working in photonics and optical communications will find this book a valuable resource.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Laszlo Gyongyosi and Sandor Imre (2012). Secure Long-Distance Quantum Communication over Optical Fiber Quantum Channels, Optical Fiber Communications and Devices, Dr Moh. Yasin (Ed.), ISBN: 978-953-307-954-7, InTech, Available from: http://www.intechopen.com/books/optical-fiber-communications-and-devices/secure-long-distance-quantum-communication-over-optical-fiber-quantum-channels

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen